DFAS 3020.26-R
DEFENSE FINANCE AND ACCOUNTING SERVICE

CORPORATE CONTINGENCY PLAN

DEFENSE FINANCE AND ACCOUNTING SERVICE

MAY 1997

FOREWORD

Each Department of Defense (DoD) Agency is responsible for developing and implementing decisive and effective contingency plans. Herein is the Defense Finance and Accounting Service (DFAS) Corporate Contingency Plan and the requirements regarding continuity of operations and support of contingency operations and mobilization. Therefore, it is incumbent upon everyone in this Agency to understand the contents and requirements of this document and prepare to support any crisis or national emergency.

Continuity of Operations Planning (COOP) is an essential best business practice to ensure DFAS can continue to meet commitments to our customers. If we do not have viable plans in place to respond to a disaster and quickly resume business, we fail in our responsibility to our customers. This document provides guidance on COOP and outlines Agency policy on the use of the automated software tool for COOP; the Living Disaster Recovery Planning System (LDRPS). It is everyone’s responsibility to give a high priority to developing and maintaining viable and fully tested plans to support COOP.

DFAS plays a major role in support of deployed forces and during mobilization. Although we do not have military forces assigned to the Agency that deploy to support contingency operations, DFAS is responsible for the financial systems and finance and accounting policy necessary to support operations. Continual planning for support of the Services during contingency operations and mobilizations is essential to ensure we provide our customers the best possible support during a time of crisis.

Questions, suggestions, or clarifications to this regulation should be directed to the Headquarters Deputy Director for Plans and Management (DFAS HQ/M).

//S//
Richard F. Keevey
Director

Distribution: A

TABLE OF CONTENTS

APPENDICES

FIGURES

REFERENCES

(a) DFAS Regulation, 3020.26-R, “Corporate Contingency Plan” November 12, 1992

(b) Executive Order 12656, "Assignment of Emergency Preparedness Responsibilities," November 23, 1988

(c) DoD Directive 3020.26, "Continuity of Operations Policies and Planning," May 16, 1995

(d) DoD Directive 3020.36, "Assignment of National Emergency Preparedness (NSEP) Responsibilities to DoD Components," November 2, 1988

(e) DoD 3020.36-P, "DoD Master Mobilization Plan (MMP)," May 1988

(f) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

(g) DFAS Regulation 8000.1-R, Information Management Policy and Instructional Guidance, August 21, 1996

(h) LDRPS Users Guide and LDRPS Administers Guide, DFAS-3020.26, Supplement 1, To Be Published

(i) LDRPS Training Guide, To be published

(j) DoD Directive 1235.11, "Management of Individual Mobilization Augmentees," January 17, 1989

(k) DFAS 1300.1M, "Military Personnel Regulation", February 1995

(l) DoD Directive 2000.12, "DoD Combating Terrorism Program," September 15, 1996

(m) DoD Directive 3020.4, "Order of Succession to Act as Secretary of Defense", July 3, 1996

(n) DFAS Regulation 5015-R, “DFAS Records Management Program,” August 1996

(o) DoD Directive 5118.5, "Defense Finance and Accounting Service," November 26, 1990
(p) DoD Directive 1200.7, "Screening the Ready Reserve," April 6, 1984

(q) DoD Directive 1235.11, “Management of Individual Mobilization Augmentees (IMAs),” May 6, 1996

(r) DoD Directive 1352.1, "Management and Mobilization of Regular and Reserve Retired Military Members," March 2, 1990

(s) DoD Directive 1400.31, "DoD Civilian Workforce Contingency and Emergency Planning and Execution," April 28, 1995

(t) DoD Directive 1100.18, "Wartime Manpower Mobilization Planning," January 31, 1986

(u) DoD Instruction 1100.19, "Wartime Manpower Mobilization Planning Policies and Procedures," February 20, 1986

(v) DoD 1100.19-H, "Wartime Manpower Mobilization Planning Guidance," March 1990

(w) DoD Instruction 3020.37, "Continuation of Essential DoD Contractor Services During Crisis," November 6, 1990

(x) DoD Instruction 3020.38, "Promulgation and Administration of OSD Crisis Action Packages (CAPs)," December 13, 1990

DEFINITIONS

1. Alternate Headquarters. An existing headquarters of a DoD Component or subordinate command designated to assume the responsibilities and functions of another headquarters under prescribed emergency conditions.

2. Alternate Files. Essential directives, instructions, programs, plans, emergency action procedures, and other documents required for the conduct of essential functions in a national emergency situation. Maintained at the alternate or relocation site.

3. CINCFORSCOM. Commander-in-Chief of the U.S. Forces Command who commands five Continental U.S. Armies (CONUSAs) and is responsible for the defense of the Continental United States.

4. Contingency. An emergency caused by natural disasters, terrorists, subversives, or by military operations. Due to the uncertainty of the situation, contingencies require plans, rapid response, and special procedures to ensure the safety and readiness of personnel, installations, and equipment.

5. Continuity of Operations. The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a mission in carrying out the national military strategy.

6. Continuity of Operations Plan (COOP). A DoD Component’s written policies and procedures to ensure continuity of operations.

7. Crisis Action Package (CAP). A set of documents that facilitate the assembly of essential elements of information and provides specific guidance on likely issues and decisions that could confront the Secretary of Defense and other OSD officials during a crisis. Each CAP contains background information on legal authorities and coordination requirements as well as draft copies of specific implementing documents that can be quickly adapted in response to an emergency situation.

8. Crisis Coordination Group (CCG). The CCG, which is a part of the CMS, consists of DoD Component members and Civil Departments and Agencies who gather in the Crisis Coordination Center (CCC) during a crisis for disseminating and coordinating timely information on key issues.

9. Crisis Management System (CMS). The CMS is a standby system that is activated by the Under Secretary of Defense for Policy, or authorized representative, during a crisis. The CMS facilitates the staffing process, and ensures that OSD senior staff officials are provided the mechanisms and procedures essential to enable them to perform their emergency responsibilities.

10. Command Post Exercise (CPX). An exercise in which the forces are simulated, involving the commander, his staff, and communications within and between headquarters.

11. CONUSA. Continental U.S. Army, subordinate to U.S. Army Forces Command.

12. Emergency Relocation Site. A site located outside a prime target area, to which all or portions of a civilian or military headquarters may be moved. It may be inactive or on a standby basis and may be manned to provide for the maintenance of the facility, communications, and database. It should be capable of rapid activation, of supporting the initial requirements of the relocated headquarters for a predetermined period, and of expansion to meet wartime requirements of the relocated headquarters.

13. Emergency Staff Designees. Individuals or staff groups prepared, with minimal prior warning, to move to designated alternate or relocation sites, form an emergency staff, and perform essential functions.

14. Essential Contractor Service. A service provided by a firm or an individual under contract to DoD to support vital systems considered of utmost importance to the U.S. mobilization and wartime missions. That includes services provided to Foreign Military Sales customers under the Security Assistance Program. Those services are essential because of the following:

a. DoD Components may not have military or DoD civilian employees to perform these services immediately.

b. The effectiveness of defense systems or operations may be seriously impaired, and interruption is unacceptable when those services are not available immediately.

15. Essential Functions. Indispensable crisis and wartime operations of the Department of Defense.

16. Graduated Mobilization Response (GMR). The process by which the United States responds to early ambiguous or explicit warning of an emerging national security emergency, including preplanned incremental steps to react flexibly to a wide range of national security threats, and provide timely preparedness measures in the areas of force readiness, industrial base preparedness, operational requirements, and combat sustainability.

17. Level Plans. Contingency and mobilization plans at different levels of command or organization.

a. Level I. Plans developed by the Department of Defense. The DoD Master Mobilization Plan (MMP) is the first level of planning and describes what is to be done, who is to do it, and how the various tasks are carried out.

b. Level II. Plans developed by the second level of command which includes the offices within the Office of Secretary of Defense, the Joint Staff, the Military Departments, and Defense Agencies.

c. Level III. Support plans developed by the third level of command. This includes the Centers and the DFAS Headquarters as a separate and distinct organization in the support of the Corporate Contingency Plan.

d. Level IV. Support plans developed by the fourth level of command. This includes the OPLOCs and any other subordinate organization of an activity that develops a Level III plan.

18. Master Scenario Events List (MSEL). A preplanned event or task in a command post exercise used to identify an issue or validate a proposed solution to a previously identified problem.

19. Mobilization. The process by which the Armed Forces or part of them are brought to a state of readiness for war or other national emergency. This includes activating all or part of the Reserve components as well as assembling and organizing personnel, supplies, and materiel. Mobilization includes but is not limited to the following categories:

a. Presidential Selective Reserve Call-up (PSRC). Expansion of the active Armed Forces resulting from action by Congress and/or the President to mobilize Reserve Component units, individual ready reservists and the resources needed for their support to meet the requirements of a domestic emergency that is not the result of an enemy attack.

b. Partial Mobilization. Expansion of the active Armed Forces resulting from action by the Congress or by the President to mobilize 1,000,000 reservists and resources needed for their support to meet the requirements of a war or other national emergency involving an external threat to national security.

c. Full Mobilization. Expansion of the active Armed Forces resulting from action by the Congress and the President to mobilize all Reserve Component units in the existing approved force structure, all individual reservists, retired military personnel, and the resources needed for their support to meet the requirements of a war or other national emergency involving an external threat to national security.

d. Total Mobilization. Expansion of the Armed Forces resulting from action by the Congress and the President to organize and/or generate additional units or personnel beyond the existing structure and the resources needed for their support to meet the total requirements of a war or other national emergency involving an external threat to the national security.

20. Noncombatant Evacuation Operations (NEO). Operations directed by Department of State, DoD, or other appropriate authority wherein noncombatants are evacuated from areas of danger overseas to safehavens overseas or to the United States. Noncombatants include dependents of service members, civilian employees of all U.S. Government Agencies and their dependents, and military personnel specifically designated for evacuation as noncombatants.

21. Presidential Selected Reserve Call-up (PSRC). The President has the authority to activate involuntarily up to 200,000 Selected Reserve members for 270 days without the requirement for declaring a national emergency.

22. Reconstitution. Actions ordered by the surviving command authority to reestablish a damaged or destroyed headquarters with survivors of the attack or personnel from other sources, predesignated as replacements.

23. Remedial Action Project (RAP) Program. Delineation of deficiencies or shortcomings in existing policies, strategies, plans, procedures, materiel, or systems that focus on major problems with joint implication that can be corrected through specific action(s).

24. Sensitive Unclassified Information. Any information which the loss, misuse, or unauthorized access to, or modification of, could adversely affect U.S. national interest, the conduct of DoD programs, or the privacy of DoD personnel.

25. Special Facility (SF). A protected emergency site managed by Federal Emergency Management Agency (FEMA) for relocation of Federal Government personnel responsible for the centralized control and allocation of national resources. The SF provides a mechanism to respond to presidential direction, to make policy decisions, to announce decisions, and to implement them.

26. Succession of Command. A process whereby a subordinate commander substitutes for and assumes the authority, duties, and functions of a disabled senior commander.

27. State Area Command (STARC). A mobilization entity within the state national guard (NG) that is ordered to active duty when NG units in that state are alerted for mobilization. It provides for the control of mobilized NG units from home station until arrival at mobilization station. It is also responsible for planning and executing military support for civil and land defense plans under the area commander.

ABBREVIATIONS AND/OR ACRONYMS

ADP	Automated Data Processing
AIS	Automated Information System
ART	Automated Information System Recovery Team
BIA	Business Impact Analysis
CAP	Crisis Action Package
CART	Crisis Action Recovery Team
CCC	Crisis Coordination Center
CCG	Crisis Coordination Group
CCT	Crisis Coordination Team
CDA	Central Design Activities
CET	Crisis Evacuation Team
CIK	Crypto Ignition Key
CINCFORSCOM	Commander-in-Chief of the U.S. Forces Command
CJCS	Chairman, Joint Chiefs of Staff
CMS	Crisis Management System
CMT	Crisis Management Team
CONUSA	Continental U.S. Armies
COOP	Continuity of Operations Plan
COTS	Commercial Off the Shelf
CPX	Command Post Exercise
CPWG	Contingency Planning Working Group
CRAT	Crisis Recovery Action Teams
CRT	Crisis Response Team
CST	Crisis Support Team
DAO	Defense Accounting Office
DEFCON	Defense Readiness Condition
DEPSECDEF	Deputy Secretary of Defense
DFAS	Defense Finance and Accounting Service
DFASE	Defense Finance and Accounting Support Element
DISA	Defense Information Systems Agency
DMC	Defense Mega Center
DMPO	Defense Military Pay Office
DODD	Department of Defense Directive
DPI	Data Processing Installation
DRP	Disaster Recovery Plan
EAT	Emergency Action Team
ECT	Emergency Coordination Team
EET	Emergency Evacuation Team
EO	Executive Order
ERAT	Emergency Recovery Action Team
ERT	Emergency Response Team
ESC	Executive Support Center
EST	Emergency Support Team
ELAN	Enterprise Local Area Network
FEMA	Federal Emergency Management Agency
FOUO	For Official Use Only
FSA	Financial Systems Activity
FSO	Financial Systems Organization
GMR	Graduated Mobilization Response
GSA	General Services Administration
IMA	Individual Mobilization Augmentee
JULLS	Joint Universal Lessons Learned

JTF	Joint Task Force
LDRPS	Living Disaster Recovery Planning System
MMP	Master Mobilization Plan
MOA	Memorandum of Agreement
MRC	Major Regional Conflict
MSEL	Master Scenario Events List
NMCC	National Military Command Center
NEACP	National Emergency Authority Command Post
NEO	Noncombatant Evacuation Operations
OPLOC	Operating Location
OSD	Office of Secretary of Defense
PSRC	Presidential Selected Reserve Call-up
PTSD	Post Traumatic Stress Disorder
RA	Risk Assessment
RAP	Remedial Action Project
SEMA	State Emergency Management Agency
SF	Special Facility
SITREP	Situation Report
SLA	Service Level Agreement
STARC	State Area Command
STU-III	Secure Telephone Unit
SWAN	Secure Wide Area Net
THREATCON	Threat Condition
USD(C)	Under Secretary of Defense, Comptroller
WARMAPS	Wartime Manpower Mobilization Planning System

CHAPTER 1

GENERAL PROVISIONS

A. **PURPOSE.** This regulation establishes the Defense Finance and Accounting Service (DFAS) policies, programs, and procedures regarding contingency planning, and assigns responsibilities. Contingency planning within DFAS consists of two categories: (1) continuity of operations to include natural emergencies; natural disasters; technological disasters; and physical security threats; and (2) providing support to deployed forces; or the Agency response during a national emergency or a mobilization of reserve forces.

B. **CANCELLATION**. DFAS Regulation, 3020.26-R, “Corporate Contingency Plan”, November 12, 1992, is canceled.

C. **APPLICABILITY.** This regulation applies to DFAS-Headquarters, DFAS Centers at Columbus, Ohio; Cleveland, Ohio; Denver, Colorado; Indianapolis, Indiana; and Kansas City, Missouri; (hereafter referred to collectively as "Centers"), organizations under the jurisdiction of the Centers (Operating Locations (OPLOCs), Defense Accounting Offices (DAOs)/Defense Military Pay Offices (DMPOs) and any other subordinate organizations), Finance Support Organizations (FSO), Financial Systems Activities (FSA) and any other DFAS organization.

D. **POLICY**.

1. Presidential Executive Order (EO) 12656 directs all levels of government to meet essential defense and civilian needs during any national emergency. Further, national emergency preparedness planning includes:

a. Identification of functions performed during an emergency.

b. Development of plans for performing the required functions.

c. Development of the capability to execute emergency plans. Create plans for the worst case scenario without the current resources available to provide support.

d. Write plans from the perspective of when, not if, a disaster occurs.

2. In compliance with EO 12656 and Department of Defense (DoD) policy and requirements per DoD Directive 3020.26, DoD Directive 3020.36, and DoD 3020.36-P, DFAS shall:

a. Develop, maintain, and exercise contingency plans to ensure that essential functions and operations continue with minimal impairment during any local or national emergency.

b. Plan for continuity of operations for any national emergency situation, to include: nuclear and non-nuclear attacks, threats of attacks, international crisis, natural and technological disasters, civil disturbance, and terrorism.

c. Develop contingency plans which are sufficiently flexible to take full advantage of any warning that could precede a national emergency, and which address the entire spectrum of conflicts and crisis.

d. Develop a corporate contingency plan (Level II) with subordinate supporting plans (Level III and Level IV) in support of DoD continuity of operations, mobilization, and wartime requirements.

e. Develop, as needed, and in coordination with appropriate DoD Components, Crisis Action Packages (CAPs) required to effect anticipated decisions and actions during continuity of operations, mobilization, and wartime.

f. Establish the optimal organizational or command structure for ensuring continuity of operations.

g. Develop plans that incorporate the use of alternate headquarters as well as emergency relocation sites.

h. Support the Office of Secretary of Defense (OSD) Crisis Management System (CMS).

i. Coordinate contingency plans within and between DoD Components, and with appropriate Federal agencies and organizations.

3. In support of the above, it is DFAS policy to:

a. Protect automated data processing by backup plans, programs, and procedures to include making, storing, and recovering of files and tapes.

b. Design and regularly test all planned and operational automated information systems to ensure that these systems can support the contingency planning requirements detailed in this document, DoD regulations, and any supplementary plans issued by DFAS-Headquarters and the Centers.

c. Provide funding resources to support the planning, maintenance, testing, and execution of contingency plans outlined in this regulation. Defense Information Systems Agency (DISA) will fund contingency plans for automated data processing requirements under its jurisdiction.

d. Establish an Agency-wide Contingency Planning Working Group (CPWG) to continually review DoD contingency planning policies, requirements and develop appropriate plans for DFAS-Headquarters and the Centers. A senior staff member assigned to the DFAS-Headquarters Deputy Director for Plans and Management, will chair the CPWG, which will meet at least semiannually, and consist of at least one representative from each Center and DFAS-Headquarters Deputy Directors' office. Representatives from DISA and other DoD Components may participate in the Agency CPWG to fully integrate and coordinate contingency plans.

e. Review and update annually the Corporate Contingency Plan (Level II) and support plans (Level III and Level IV) developed by DFAS-Headquarters, the Centers and OPLOCs.

f. Classify, as appropriate, per DoD directives and instructions, those plans dealing with relocation sites and procedures.

g. Test contingency plans to ensure the Agency's support and execution of DoD's continuity of operations, mobilization, and war plans. DFAS-Headquarters and the Centers will participate in and fully support the Chairman, Joint Chiefs of Staff (CJCS) command post exercises and other evaluations.

E. **RESPONSIBILITIES**.

1. The DFAS-Headquarters Deputy Directors and General Counsel shall:

a. Ensure consideration of the Agency's responsibilities and functions delineated in DoD Directive 5118.5 during all phases of contingency planning, and executed during continuity of operations, mobilization, and wartime.

b. Assist the DFAS-HQ Deputy Director for Plans and Management in developing and implementing the Corporate Contingency Plan (Level II) and DFAS-Headquarters Contingency Support Plan (Level III).

c. Develop and implement the various contingency support programs identified in this regulation.

2. Specific responsibilities assigned to the DFAS-Headquarters include the following:

a. The DFAS-Headquarters Deputy Director for Plans and Management shall:

(1) Ensure the implementation of this regulation and give advice and guidance to each DFAS Center related to contingency planning.

(2) Establish a corporate Crisis Management System (CMS) with the requisite plans and components as outlined in chapter 2, and ensure that the DFAS CMS integrates into and supports the OSD CMS.

(3) Develop and maintain a Level III contingency plan for DFAS-Headquarters that implements the Corporate Contingency Plan.

(4) Formulate appropriate actions for the Director’s approval, in coordination with the DFAS-Headquarters Deputy Directors, regarding changes in the Defense Readiness Conditions (DEFCON).

(5) Establish plans and procedures for DFAS to fully support and participate in the Chairman, Joint Chiefs of Staff (CJCS) Command Post Exercise (CPX) Program, and:

(a) Institute a corporate Remedial Action Project (RAP) program and maintain a current automated data processing (ADP) database of RAPs.

(b) Coordinate the Agency participation in the CJCS Joint Universal Lessons Learned (JULLS) program and be responsible for the associated ADP software support requirements.

(c) Submit appropriate corporate RAPs for inclusion in JULLS.

(6) Formulate plans and procedures in support of the OSD and DFAS Crisis Action Package (CAP) program.

(7) Develop and publish an annual contingency test and exercise plan, in coordination with the Military Services, the Joint Staff, DISA, and Centers.

(8) Maintain current information on essential contractors providing services to DFAS activities.

b. The DFAS-Headquarters Deputy Director for Resource Management shall:

(1) Manage the DFAS Selected Reserve Augmentation program.

(2) Identify on DFAS personnel manning documents, in coordination with Headquarters Deputy Directors and Center Directors, the DFAS key billets for mobilization purposes.

(3) Develop, in coordination with DFAS-Headquarters Deputy Director for Plans and Management, a DFAS Wartime Manpower Mobilization Planning System (WARMAPS).

(4) Develop and implement an Agency terrorist Threat Condition (THREATCON) System.

(5) Develop policies and procedures in support of Continuity of Operations Planning (COOP) to include:

(a) Records management, including vital records.

(b) Finding replacement facilities.

(c) Obtaining contingency contracts.

(d) Safety deficiency triage.

(e) Emergency funding authority.

(f) External Services (Public Affairs, Congressional Liaison Office, etc.).

c. The DFAS-Headquarters Deputy Director for Human Resources shall:

(1) Develop plans and procedures regarding work stoppage.

(2) Formulate plans and procedures to preclude assignment of military reservists and retirees to key billets

which would adversely impact DFAS operations should they be recalled to active duty in support of mobilization.

(3) Develop procedures and notify the immediate family members of DFAS employees who are fatalities or serious injuries.

(4) Formulate COOP policies and procedures for personnel accountability, furloughs, and emergency leave.

d. The DFAS-Headquarters General Counsel shall: Review all contingency plans to ensure compliance with statutes and regulations regarding emergency authorities and assist in developing contingency or emergency legislation.

e. The DFAS-Headquarters Deputy Director for Information Management shall:

(1) Develop and distribute policy standards/guidelines for ensuring backup capability of DFAS automated information systems, databases, software parameters/files, etc., and provide oversight for off-site storage of the required backup files on a regularly scheduled basis. Backup files of computer data are required for recovery of mainframe, mid-tier, wide or local area network operating environments, and personal computers that support time-sensitive business operations.

(2) Formulate policies and procedures for the security of Automated Information Systems.

(3) Negotiate annual Service Level Agreements (SLA) with DISA and ensure it includes provisions for COOP and perform liaison within that agency.

(4) Participate in the development and execution of Agency COOP procedures and testing.

3. Center Directors shall:

a. Comply with the provisions of this regulation and develop plans (Level III) with supporting programs and procedures that implement the Corporate Contingency Plan.

b. Establish a Center CMS with requisite plans, programs, procedures, and equipment that integrates into and supports the DFAS corporate CMS.

c. Ensure that OPLOCs, DAO/DMPOs or remote sites under their purview have appropriate contingency plans, programs, and procedures.

d. Forward proposed contingency and support plans to the DFAS-Headquarters Deputy Director for Plans and Management for review and approval before promulgating such plans.

4. OPLOC Directors shall:

a. Comply with the provisions of this regulation and develop plans (Level IV) with supporting programs and procedures that implement the Corporate and parent Center's Contingency Plan.

b. Establish an OPLOC CMS with requisite plans, programs, procedures, and equipment that integrates into and supports the DFAS corporate CMS.

c. Forward proposed contingency and support plans to their parent Center for review and approval before publishing such plans.

F. **EFFECTIVE DATE**. This regulation is effective immediately and is mandatory for use by all staff assigned to the DFAS-Headquarters, Centers and OPLOCs.

CHAPTER 2

CRISIS MANAGEMENT SYSTEM

A. GENERAL. The Corporate Contingency Plan consists of various planning elements or requirements. The key to execution of the plan is an Agency-wide Crisis Management System (CMS). The CMS is the framework to provide management with information to make timely informed decisions and expedite the flow of information between DFAS-Headquarters, subordinate Centers and OPLOCs and an interface with the Office of the Secretary of Defense. The system establishes procedures for immediate notification of the DFAS-Headquarters, Centers, and/or appropriate Agency personnel if a local disaster, national emergency or an impending situation occurs that could affect a mission or function. Further, the Agency Crisis Management System interfaces with similar management systems within the Office of Secretary of Defense, the Joint Staff, other Defense Department Components, Federal Agencies and organizations to coordinate and exchange information.

B. CRISIS MANAGEMENT SYSTEM (CMS).

l. The CMS is a standby system activated in response to a crisis, emergency, national security event, or training exercise. Events occurring locally, nationally or internationally could cause the activation of the CMS. The purpose of the CMS is to:

a. Disseminate essential information to the Agency leaders and/or higher level decision makers.

b. Create a mechanism for the flow of significant or rapidly changing information from DMPO/DAO/OPLOCs, to Centers, to DFAS-Headquarters, and to higher headquarters (Joint Staff, USD(C) and OSD CMS), and vice versa.

c. Coordinate single or multiple actions which could be time sensitive, especially in an actual crisis.

d. Resolve issues at the lowest appropriate levels of the Agency.

e. Facilitate the staffing process and provide senior agency command leaders with information, mechanisms, and procedures essential to discharge their emergency management responsibilities.

2. Office of Secretary of Defense (OSD) CMS.

a. This Agency, per DoD Directive 3020.36, shall support and participate in the OSD CMS. An element of this management system is the OSD Crisis Coordination Group (CCG). This Group, made up of selected DoD leaders and staff members with TOP SECRET clearances, meets in the OSD Executive Support Center (ESC) during emergencies for the rapid dissemination and coordination of timely information on key issues at the highest DoD level.

b. The DFAS-Headquarters Deputy Director for Plans and Management, with the assistance of DFAS-Headquarters Deputy Directors and General Counsel, shall organize and formulate plans for the Agency's support of the OSD CMS and participation in the OSD ESC.

c. The Agency Director, Principal Deputy Director, Deputy Directors, General Counsel, and support staff consisting of at least one person from each Deputy Director's office will have a TOP SECRET clearance and access to ensure the Agency can support full participation in the OSD CMS.

3. DFAS CMS.

a. General. An Agency-wide CMS provides appropriate crisis and emergency responses to the OSD ESC, and within the Agency. The Agency Director or Principal Deputy Director may partially or fully activate the Crisis Management System. A Center or OPLOC Director may activate his/her CMS based on local emergency circumstances, or for training and testing.

b. Crisis Coordination Centers. DFAS-Headquarters, Centers and OPLOCs will establish CCCs which are the focal points for the command and control of the CMS. Each CCC is a separate facility, office, or conference room that has the appropriate level of security and control to permit SECRET level communications and large enough to handle the requisite equipment and support staff. An OPLOC CCC provides the interface with the Center CCCs. A Center CCC provides the interface with the DFAS-Headquarters CCC which links in turn to the OSD CCC, as required by the situation. The satisfactory completion of the following CCC requirements will provide essential operations and communications throughout the Agency.

(1) Operations. The DFAS-Headquarters, Center and OPLOC CCCs can become operational on instant notification with pre-designated and thoroughly trained personnel and the requisite CCC equipment. Local emergencies, crisis, other real world events, training, and exercise participation may require limited personnel support or the full utilization of all designated CCC personnel. Hours may vary from normal duty hours to an expanded 24 hour operations. Every CCC will have a designated director (an additional duty) who is responsible for the crisis center operations and functions.

(2) Alternate and Backup Facilities. DFAS-Headquarters, Centers and OPLOCs will make plans to activate an alternate or backup CCC in the event the primary CCC is not available. This facility must be capable of supporting CCC operations for at least the first 48 hours of a crisis. Store excess secure equipment in this facility or develop contingency plans for the emergency procurement of the requisite CCC equipment.

(3) Requisite Equipment. The equipment in the CCC must consist of operational Secure Telephone Unit (STU-III) communications to include one unit for the secure computer and another for secure facsimile and secure voice. Each CCC must have a secure computer capable of processing classified information (up to SECRET) that complies with security standards, a paper shredder, and a security container (safe) for storage of SECRET material. The local security manager must certify placement and use of this equipment.

(4) Security of STU-III Crypto Ignition Keys (CIKs). When separated from the secure telephone unit in support of the CCC, handle the CIK as a high value item and protect at the same level as the keying material. To ensure that the keys are available to the proper CCC personnel, store the CIKs in an approved security container, accessible for all CMS requirements. In addition, a minimum of three people should have access to the security container and CIKs.

(5) Personnel Security Clearances. Plan to execute CCC functions at the SECRET level of classification. Therefore, sufficient numbers of staff action personnel and support members must have the proper security clearance/access to stand around-the-clock watches, work issues by functional area, and provide responses to higher headquarters. Permit only people certified with at least a SECRET security clearance in the CCC during classified operations.

(6) Personnel Qualifications. Pre-designate and train qualified personnel to support and participate in the CCC operations. These personnel should prepare to react to an immediate crisis. Every CCC must have a core of personnel, capable of handling various tasks during a crisis including operating the equipment, providing administrative support, coordinating responses to inquires, and standing watches.

c. Situation Reports (SITREPs). Centers shall submit a SITREP to the DFAS-Headquarters CCC, and DFAS-Headquarters to appropriate CCCs, when unusual circumstances or unplanned emergency events occur. In all cases, it is prudent to "over report" to keep the Agency leaders informed rather than to delay or not report problems on less than satisfactory situations as they occur. Appendix A provides instructions on the submission of SITREPS.

d. Planning Requirements. DFAS-Headquarters, Centers and OPLOCs shall develop plans, with implementing programs and procedures, that delineate the CMS operations and requirements. Along with the CCC and SITREP requirements discussed above, the plan will include operating instructions that cover the normal daily CCC operation and those activities initiated upon activation of the CMS. These instructions must contain sufficient details to permit a smooth, instantaneous activation of the CCC when required by higher authority or local situations, and include the following:

(1) CCC Recall Roster. An updated roster to include office and home telephone numbers of all people qualified and trained in the operation and function of the CCC. Conduct periodic training of these personnel on CCC operations during emergency situations.

(2) Key Personnel. Maintain a current roster of key, essential personnel in each functional area, as determined by each organization, with office and home telephone numbers in the CCC or accessible to those staffing the CCC.

(3) Personnel Notification Procedures. Some OPLOCs/Centers may need to notify large numbers of essential personnel in the recovery, relocation or reconstitution of essential functions. Therefore, each Center should have explicit instructions for the notification of essential people within each directorate/section during off duty hours. Additionally, maintain the home telephone numbers of ALL military personnel in the CCC, or accessible to CCC personnel,

for possible family emergency notification requirements. Comply with the provisions of the Privacy Act regarding the handling of this information.

(4) Checklists. Develop and use crisis action checklists to provide a systematic plan for dealing with an emergency to include details on completing all possible requirements. Checklists will include functional areas such as Agency notification; organization personnel, public affairs; logistics including supply, travel, and equipment, and physical security.

(5) Automated Information System (AIS). Formulate an AIS security plan for the CCC that complies with the requirements of DoD Directive 5200.28 and DFAS Regulation 8000.1-R. These references require that an AIS for processing classified or sensitive unclassified information must meet minimum requirements. These requirements include: accountability; access; security training and awareness; physical controls; markings; data continuity; contingency (backup) planning; accreditation; and risk management. In addition, isolate the AIS used for classified matters electronically, logically, and physically from all personnel and information systems not possessing the requisite clearance or authorization. Develop and document detailed operating instructions to clearly show the performance of secure AIS operations.

(6) Log. Maintain a log when activating the CMS. The log is an official document listing the watch standers and describing the events and actions as they unfold.

(7) Tests and Evaluation. Periodically validate the anticipated crisis actions to ensure that proper and correct plans and procedures are in place. Therefore, at least every six months, test the emergency recall roster and ensure personnel notification procedures are current during a normal off duty time period. Evaluate emergency team procedures and emergency checklists annually.

e. Memorandum or Letter of Agreement. Develop written support agreements, as required, with another DoD Component or local security force to ensure notification of key leaders or other appropriate people during off duty hours. The appropriate Agency leaders must approve the agreements.

f. Selected Reserve Augmentation. The CCC requires around-the-clock manning only during a crisis, emergency, mobilization, exercise, or testing period. Selected Reserve members could become key members for the CCC's administrative and operational functions. Drilling reservists are a trained force that can develop contingency plans and procedures and ensure that a qualified staff is immediately available for all possible contingency scenarios and CCC operations. They provide a trained resource familiar with crisis situations, eliminating the need to hire and train new civilian staff members during an emergency. For these reasons, the Headquarters and Centers are encouraged to use Individual Mobilization Augmentees (IMAs), or in the case of the Navy, reserve units, in support of the crisis management system personnel requirements. The DFAS-Headquarters Deputy Director for Resource Management manages the IMA program as prescribed in DoD Directive 1235.11 and DFAS 1300.1M.

C. **EMERGENCY ALERT NOTIFICATION CONDITIONS**.

1. Use alert, threat, defense, and other "condition" code words to notify the affected DFAS organization based on specific emergency scenarios. These code words are standard throughout DoD and other Federal Agencies and used in all types of contingencies including continuity of operations, mobilization, and wartime. In some cases, DFAS Centers and activities may be notified by a Federal Agency or other DoD Component of emergency situations and alert conditions before such circumstances are known by DFAS-Headquarters. When this occurs, notify DFAS-Headquarters by a SITREP.

2. Terrorist Threats Against Facilities and People. Terrorist attacks will likely occur with little or no warning. Since DFAS-Headquarters, Centers and remote activities are not in proximity but located in different areas of varying degrees of potential threats, each organization must determine its level of risk and establish appropriate anti-terrorism procedures. DoD Directive 2000.12 delineates these procedures and the specific measures to take. The DFAS-Headquarters Deputy Director for Resource Management and Center Directors shall develop and implement a terrorist Threat Condition (THREATCON) System based on this DoD directive. Furthermore, base any action in response to terrorism on all appropriate sources of information including intelligence reports, local/state law enforcement information, and liaison with other local, state, and/or federal agencies, but tempered by best judgment and knowledge of the local situation. In all cases, submit a SITREP whenever increased security measures are taken in response to terrorism. Following are the code words used to identify THREATCONs in the DoD directive:

a. THREATCON NORMAL. This condition applies when a general threat of possible terrorist activity exists, but warrants only a routine security posture.

b. THREATCON ALPHA. Nonspecific threat(s) of terrorism against U.S. military and civilian personnel or facilities in a general geographic area. The nature and extent of a terrorist activity within this threat condition are unpredictable. However, it may be necessary to implement certain measures as a result of intelligence reports or as a deterrent.

c. THREATCON BRAVO. More predictable threat(s) of terrorism against U.S. military and civilian personnel or facilities exist within a geographic area. Plan to maintain the measures in this threat condition for weeks without causing undue hardship, affecting operational capability, or aggravating relations with local authorities.

d. THREATCON CHARLIE. Imminent threat of terrorist acts against specific U.S. military and civilian personnel or facilities. Implementation of the measures in this THREATCON for more than a short period may create hardship and affect the peacetime activities of the unit and its personnel. The threatened organization will activate the CMS when this threat condition is in effect.

e. THREATCON DELTA. This condition applies when a terrorist attack occurs in the local area or the command receives information that terrorist action against a specific location is likely. Normally, declare this THREATCON as a localized warning.

3. Attack on the Continental United States.

a. Readiness Condition.

(1) Condition ALPHA. Assumes that a surprise attack (generally considered to be a nuclear attack) will destroy or limit the use of normal, daily facilities with such suddenness that relocation before the attack cannot take place. Planning for condition ALPHA shall incorporate use of existing facilities, designation of alternate headquarters and successors.

(2) Condition BRAVO. Assumes that there will be sufficient time before an impending attack for the emergency staff personnel to relocate. All Agency Components will initiate plans to activate the emergency relocation site.

b. During a period after an attack, give priority to military operations and logistical support, maintenance and restoration of law and order, support of civil defense, and damage and residual resource assessment. Initial actions shall focus on survival activities, military operations, mobilization of military and civilian manpower as required, restoration of essential communications, transportation, and performance of other essential functions. Over the longer term, restructure and restore headquarters staffs, capabilities, and functions as resources permit. Plans to reconstitute DoD finance and accounting functions on a case-by-case basis depending on cost and resources.

4. Defense Readiness Conditions (DEFCON). A uniform system of progressive alert postures identified by the acronym DEFCON and a number 1 to 5. Public announcement of a DEFCON shall follow Presidential decisions and guidance from the Secretary of Defense issued under the various conditions. The DFAS Director will determine required actions within the Agency for each DEFCON at the time readiness conditions change. Defense readiness conditions are as follows:

a. DEFCON 5. Normal readiness.

b. DEFCON 4. Increase intelligence watch and strengthen security measures.

c. DEFCON 3. An increase in force readiness above that required for normal readiness.

d. DEFCON 2. A further increase in force readiness, but less than maximum readiness.

e. DEFCON 1. Maximum readiness.

5. Civil Alert Conditions. In an emergency, remote DoD organizations and those collocated with another Federal Agency or not located on a military installation, may receive official readiness instructions from the President or the Director, Federal Emergency Management Agency (FEMA). The readiness instructions not related to DEFCONs are provided for information purposes only. The following are the readiness levels for civil preparedness actions:

a. Communications Watch. Establish a capability to monitor official communications channels on a 24-hour per day basis wherever such a capability is lacking. Implement this alert condition without public disclosure and with a minimum of internal disclosure.

b. Initial Alert. Staff emergency operating centers at regular national offices continuously. Extend communications watch to regional and other major field offices. Curtail or suspend some regular agency activities as necessary.

c. Advance Alert. A general and public participation in emergency and civil preparedness actions to achieve the highest degree of civil emergency readiness. Complete actions necessary for activation of alternate emergency operating centers. Receive emergency duties including continuation of the essential processes of government as well as emergency preparations for the essential functions required if warning of attack.

D. **RELATIONSHIPS WITH GOVERNMENT AGENCIES**. DFAS-Headquarters, Centers, and other activities will develop working relationships with government agencies at the national, state, and local level that have similar crisis management responsibilities. Most government agencies engage in disaster or emergency planning activities and participate in joint agency planning meetings. These meetings provide a means of sharing ideas and establishing a network of knowledgeable people for resolving actual emergencies. Therefore, it is important to establish these relationships and foster inter-governmental planning and mutual support.

CHAPTER 3

CONTINUITY OF OPERATIONS

A. GENERAL. Continuity of Operations Planning (COOP) is essential to ensure DFAS can continue to meet commitments to our customers. The primary objectives of COOP are to safeguard personnel, protect DFAS assets, manage risk, avert or lessen the impact on operations of an adverse situation, provide for timely resumption and continuation of operations, and maintain adequate service levels for our customers. This includes recovery from an emergency that adversely affects personnel, automated information systems, facilities, or equipment of any DFAS organization. It also includes taking preventive measures and actions that will decrease the possibility or the impact of an adverse incident and protect life, information, and physical assets. If an emergency should occur, the Agency must have viable contingency plans in place to enable effective and efficient response, immediate resumption of time critical business functions, recovery of less time sensitive business functions, and reconstitution of normal operations. This includes the capability to contact or account for employees as well as relocating operations to an alternate (local area) or backup (non-local area) site. Each organization within DFAS must develop a program with detailed procedures to provide current, critical information so all individuals know what to do, when and where to go, and how to get there. Regularly rehearse these COOP plans and test to ensure the policies, procedures, and actions are viable and personnel can successfully manage unexpected situations. By far, COOP is the most important category of contingency planning in maintaining operations for the DoD finance and accounting community.

B. CONTINUITY OF OPERATIONS PLANNING (COOP).

1. Basic COOP Concepts and Strategies. Responding to actual emergency scenarios in which unanticipated events occur requires flexible COOP plans. An emergency that disrupts normal operations can occur at any time and place with varying degrees of impact. In most cases, the emergency is limited in scope and magnitude. However, DFAS COOP plans must address the worst possible scenario as well as situations with lesser degrees of disruption and destruction. Since it is not possible to document every possible contingency scenario, develop flexible COOP plans to respond to varying degrees of impact based on destruction, duration, time-sensitive operations, and geographic scope, etc.

a. Contingency Scenarios. Address at least the seven basic contingency scenarios:

(1) Evacuation of a facility (or a portion of the facility) during an emergency and the response to assess the situation and reestablish operations.

(2) Emergency procurement of supplies, equipment or services.

(3) Relocation of all or part of the operation to a local (alternate) site.

(4) Relocation of all or part of the operation to a non-local (backup) site.

(5) Assist DISA in the relocation of data processing support from a supporting Defense Mega Center to an alternate or backup facility.

(6) Reconstitution of all operations at a new location.

(7) Increased requirements to support the Services during a mobilization including the operational impact of the potential loss of DFAS active duty military or the activation of DFAS civilian employees who are reserve military personnel.

b. Protection of DFAS Resources. Provisions for protecting DFAS personnel and other resources are an important part of COOP. This includes preventive measures such as off-site storage of vital records, evacuation procedures, emergency notifications, and accountability of personnel.

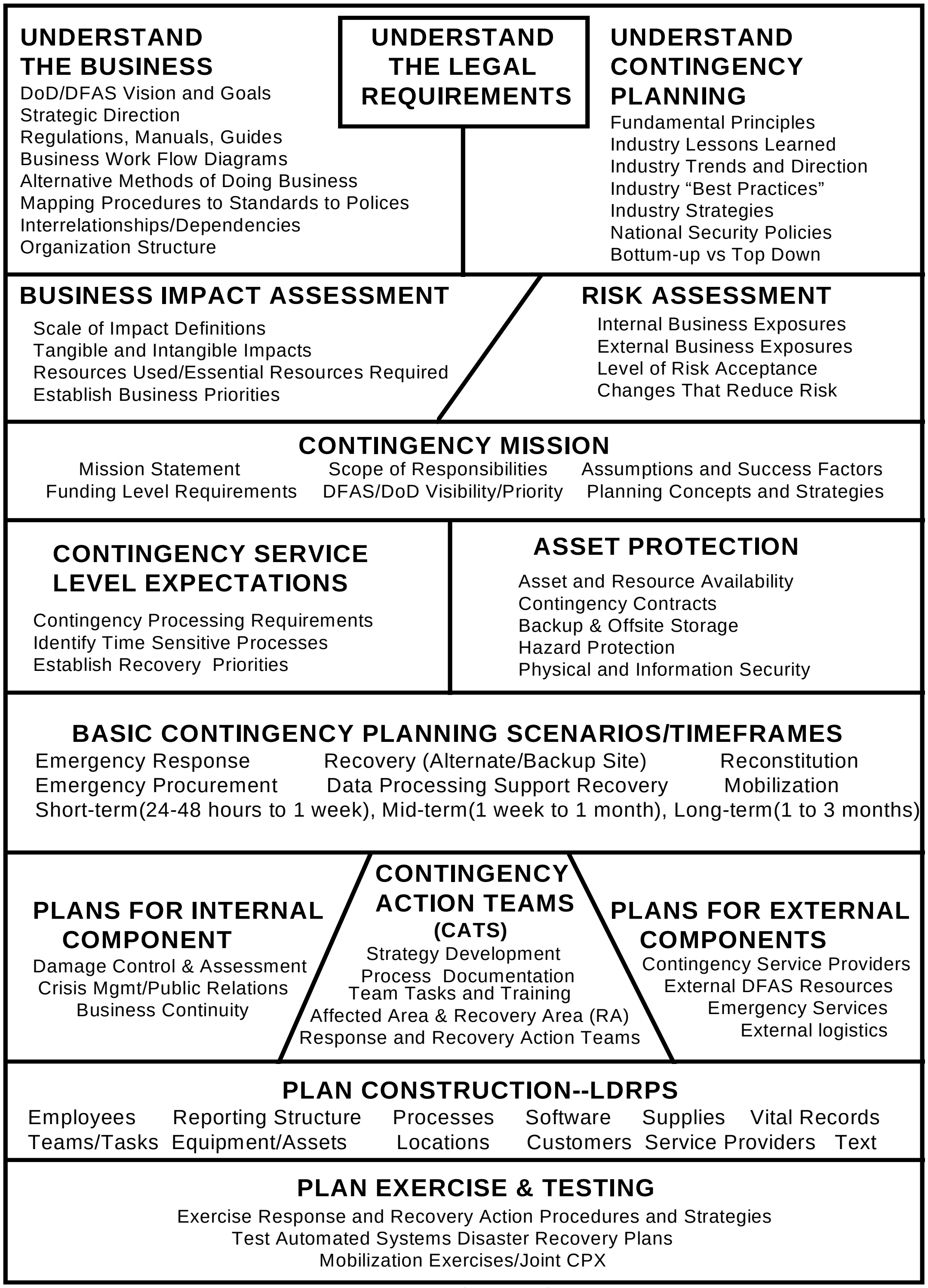
c. Relocation. It is significantly more difficult to move operations out of the local area, however, most facility arrangements provide for emergency local facility replacement and organizations only develop plans for emergency relocation to an alternate (local) site. This type of planning must occur, however, DFAS organizations must also develop COOP plans for relocation outside the local area to a backup (non-local) site for contingency situations that require movement outside the geographic area. If possible, plan to relocate to another DFAS facility to facilitate reestablishing connectivity.

d. Limited Operations. Include realistic requirements for prioritizing and scaling back operations to only essential processes, personnel, and other resources during a recovery. As a minimum, COOP plans must cover the time-span of requirements for immediate response, short-term (24-48 hours to one week), mid-term (one week to one month), and long-term (one to three months) recovery, as well as full reconstitution of operations (three months). Identify time-sensitive critical processes, emergency personnel, priorities for recovery, and dependent operations. In addition, COOP plans must include procedures for timely notification, response, and recovery of critical time sensitive operations.

e. Planning Cycle. The COOP planning cycle is shown at Figure 3-1.

2. COOP Plan Organization. Use the Living Disaster Recovery Planning System (LDRPS) software tool to document DFAS COOP plans. The COOP plan consists of text files for “static” information (information that does not change very often) and a database to contain “dynamic” information (information that changes more frequently, but also information available for extraction in a number of different ways from the database). The “static” portion of the COOP plan constitutes the basic COOP plan and is attached as a text file in LDRPS. Also attach information that is too voluminous to include in the LDRPS database as a text file. This includes word-processing files, spread-sheets, and pictures or objects such as maps. The “dynamic” information will augment the basic COOP plan “as needed” based on the applicable contingency scenario by extracting information from the LDRPS database using standard or customized reports.

DFAS CONTINGENCY PLANNING APPROACH



UNDERSTAND THE BUSINESS
DoD/DFAS Vision and Goals
Strategic Direction
Regulations, Manuals, Guides
Business Work Flow Diagrams
Alternative Methods of Doing Business
Mapping Procedures to Standards to Polices
Interrelationships/Dependencies
Organization Structure

UNDERSTAND THE LEGAL REQUIREMENTS

UNDERSTAND CONTINGENCY PLANNING
Fundamental Principles
Industry Lessons Learned
Industry Trends and Direction
Industry "Best Practices"
Industry Strategies
National Security Policies
Bottum-up vs Top Down

BUSINESS IMPACT ASSESSMENT
Scale of Impact Definitions
Tangible and Intangible Impacts
Resources Used/Essential Resources Required
Establish Business Priorities

RISK ASSESSMENT
Internal Business Exposures
External Business Exposures
Level of Risk Acceptance
Changes That Reduce Risk

CONTINGENCY MISSION
Mission Statement
Scope of Responsibilities
Assumptions and Success Factors
Funding Level Requirements
DFAS/DoD Visibility/Priority
Planning Concepts and Strategies

CONTINGENCY SERVICE LEVEL EXPECTATIONS
Contingency Processing Requirements
Identify Time Sensitive Processes
Establish Recovery Priorities

ASSET PROTECTION
Asset and Resource Availability
Contingency Contracts
Backup & Offsite Storage
Hazard Protection
Physical and Information Security

BASIC CONTINGENCY PLANNING SCENARIOS/TIMEFRAMES
Emergency Response
Recovery (Alternate/Backup Site)
Reconstitution
Emergency Procurement
Data Processing Support Recovery
Mobilization
Short-term(24-48 hours to 1 week), Mid-term(1 week to 1 month), Long-term(1 to 3 months)

PLANS FOR INTERNAL COMPONENT
Damage Control & Assessment
Crisis Mgmt/Public Relations
Business Continuity

CONTINGENCY ACTION TEAMS (CATS)
Strategy Development
Process Documentation
Team Tasks and Training
Affected Area & Recovery Area (RA)
Response and Recovery Action Teams

PLANS FOR EXTERNAL COMPONENTS
Contingency Service Providers
External DFAS Resources
Emergency Services
External logistics

PLAN CONSTRUCTION--LDRPS
Employees
Reporting Structure
Processes
Software
Supplies
Vital Records
Teams/Tasks
Equipment/Assets
Locations
Customers
Service Providers
Text

PLAN EXERCISE & TESTING
Exercise Response and Recovery Action Procedures and Strategies
Test Automated Systems Disaster Recovery Plans
Mobilization Exercises/Joint CPX

FIGURE 3-1

3. COOP Plan Administration. The DFAS functional business managers and their contingency planning staff will conduct a review of the entire COOP plan (both “static” and “dynamic” information) at least annually by September 30 of each year. Submit the results of this review to the Director of the applicable DFAS entity as well as DFAS-Headquarters Deputy Director, Plans and Management. In addition, management or contingency team members from the functional business unit will continually update “dynamic” information to ensure the COOP plan is current.

4. COOP Plan Development.

a. Essential Resources. The COOP plans should identify the full range of essential resources needed for response, recovery, and reconstitution efforts. The resource requirements should include personnel, work space, telephone, terminals, personal computers, office equipment, documents, supplies, forms, document routine processes, interaction with customers and service providers, and dependencies with other processes.

b. Recovery Strategies. Develop recovery strategies based on the worst possible scenario. Address the actions to follow if there is a disaster including operational changes of the business operations and processes. The recovery strategy should take into account the overall effect on the Agency’s operations. Develop notification lists to ensure prompt notification of employees, customers, and service providers. Identify and prioritize time sensitive functions, business processes and automated information systems. Designate backups for staffing as well as backup requirements or emergency acquisition procedures for vital records, automated information system processing, telecommunications, forms, supplies, furniture, and equipment. Document directions, transportation requirements, points of contact, services, and supplies required for emergency control (including management, coordination, reporting, and assembly), alternate operations processing (local relocation), backup operations processing (non-local relocation), and off site storage locations.

C. COOP RESPONSIBILITIES.

COOP requires the collective efforts of all personnel in an organization. Without this total effort the COOP plan will never capture all the key elements critical to developing a complete plan of action.

1. Management.

a. Senior management support and direct involvement in the planning process is essential.

b. Management throughout the organization is responsible for implementing COOP policy and procedures within their respective area of responsibility.

2. Contingency Planners.

a. The DFAS-Headquarters contingency planning staff will establish DFAS wide polices and procedures for developing, maintaining, and exercising COOP plans. The DFAS-Headquarters planning staff will maintain a centralized inventory of all COOP plans and monitor exercises. They will provide a COOP status report to the DFAS Director annually.

b. Each DFAS entity will have at least one individual designated as a contingency planner. The contingency planner(s) act as the facilitator(s) and consultant(s) for COOP plans development and testing for the entity. The contingency planner(s) is also responsible for establishing emergency (crisis) coordination and management teams' guidelines and training team members on emergency contingency responsibilities. Center and FSA contingency planners may also be delegated the responsibility for LDRPS systems administration. The system administrator is responsible for performing routine maintenance and entering changes to fields and reports, creating LDRPS reports, and providing technical support to LDRPS users.

c. Contingency Planning Working Group (CPWG).

(1) Agency. The DFAS-Headquarters contingency planning staff will establish an agency wide Contingency Planning Working Group. Personnel designated as contingency planners at each DFAS Center and FSO will participate in the Agency CPWG. This group will meet regularly to discuss issues related to contingency planning within the Agency.

(2) DFAS-Headquarters and Centers. The contingency planners for the DFAS-Headquarters staff and each Center will establish a CPWG for their activity. Each Directorate will have at least one person assigned as a representative to the entities CPWG. The members of the CPWG are responsible for overseeing the COOP plan development for their respective organizations.

3. Business Managers.

a. The business manager and their staff are the most knowledgeable of their essential processes and how to effectively recover operations. Each business manager should designate at least one individual to coordinate COOP for their major business function or organization. The business manager is ultimately responsible for performing risk assessments and developing and maintaining the detailed COOP for their business area. The business manager is also responsible for reviewing and exercising COOP plans at least annually. This includes documenting, maintaining, and exercising the COOP requirements for automated information systems (AISs) for which they are the office of primary responsibility. The business manager is also responsible for making decisions regarding the necessary preventive actions based on the Risk Assessment (RA) or Business Impact Analysis (BIA) of the operation they manage. Considering costs involved or other impact considerations, the business manager may need to elevate the decision to higher management. The business manager will establish a Crisis Action Recovery Team (CART) for managing recovery of the business area and informing team members of their responsibilities and providing training in recovery strategy and procedures. The business manager or supervisor is responsible for accountability and notification of employees in their organization during an emergency.

b. Most DFAS operations are dependent on the emergency response and recovery capability of other organizations. Therefore, COOP is a coordinated effort with organizations, both internal and external, which provide critical operations support. This includes those organizations that provide AIS support such as the Defense Information Systems Agency (DISA), DoD component Central Design Activities (CDAs), or the DFAS-FSO/FSA. Without their planning efforts and assistance we may not have the necessary systems or back up data to recover.

D. PLANNING ASSUMPTIONS. Every COOP plan includes some assumptions. Document any assumptions made in developing the COOP plan. The following are examples of some basic planning assumptions that might apply:

1. Disasters will Range From Worst Case to Less-Severe Interruptions. A worst case scenario might assume: employees incapacitated, DFAS facilities or that of the AIS service provider are totally unusable or inaccessible, and no salvageable equipment, data, documentation, etc., exists. However, more likely is a less serious interruption in-which the employees, facility, equipment, data, are available or salvageable.

2. Localized or Regional Emergencies. Most contingency situations are in one geographic area and will only affect

those DFAS entities and service providers located within that region. All other DFAS facilities are operational.

a. Local. In circumstances involving a localized event (e.g., fire in building), government agencies such as the General Services Administration and local vendors such as utility companies are able to replace or install facilities, computer and communications, power, portable water, and portable toilets , within a specified “x” to “y” time based on pre-arranged contingency contracts or procurement arrangements or agreements.

b. Regional. In the case of a regional emergency (such as a hurricane, flood, or earthquake), the time required to recover might be as long as “x” to “y” weeks. This is due to multiple municipalities, services, facilities, and businesses contending for the limited emergency resources and services. Regional emergencies that cause wide-spread disruption of public utilities such as electricity, water and telecommunications may also cause additional delays in re-establishing operations without pre-identified or arranged alternate sites within the same region.

3. COOP Plan Documentation. If personnel who normally perform the operations are not available, the documentation in the COOP plan should enable management and staff familiar with DFAS business functions, automation technology, and the requirements of the COOP plan to recover operations.

4. Available Personnel. Sufficient management and staff, familiar with DFAS business functions and trained in procedures and tasks in this COOP plan, are available subsequent to the interrupting event to implement response and recovery efforts. In addition, the national or local economy is able to meet the requirements for hiring and training new employees.

5. Vital Records. Backup and store, off site, all business documentation and files necessary for resumption and recovery for retrieval within “x” to ”y” time frame during a crisis.

6. Computer Files. Backup all computer data files required to implement recovery of mainframe, mid-tier, wide or local area network operating environments, and personal computers that support time-sensitive business operations daily or at other regularly scheduled times. Rotate these backups off-site weekly or for a pre-determined period sufficient to ensure the protection of data and applications software. The business manager must approve the type of backup; the timing of the off-site rotation; retention; and ensure the strategy will

minimize the re-entry or re-construction of data and recovery of files to status.

7. Backup Storage Locations. Store all backup items for resumption and recovery that cannot be easily and quickly obtained or created from other identified sources at on-site or off-site locations. Store backups on-site in a fire resistant safe in a location that is remote from the business and technology departments. Locate backups stored off-site outside the immediate geographic area and in an area that is not affected by the same regional disaster affecting the originating location.

8. Notifications. Document and maintain in the COOP plan all information necessary to easily and quickly complete internal and external contacts required in an emergency.

9. Contingency Funding. Contingency funding is available from existing DFAS funds or from other Defense sources for most crisis situations. Legislation or executive orders will provide authority and funds for major disasters or mobilizations.

10. Contingency Support. Service providers will honor contingency support contracts or agreements. This includes interagency agreements with DISA for AIS processing support as well as contracts with private vendors.

11. Recovery Scenarios. Depending upon the type of incident, execute COOP plans for the seven (7) basic scenarios: Document sufficient policies and procedures in the COOP plans to enable recovery of all essential business functions including special and unique processes. Procedures and policies will be in place to suspend nonessential procedures.

12. Recovery Time Frames. DFAS business managers determine the time for recovery of each business function or process and ranges from 24 hours to 3 months (90 days). Identify the mission criticality and resumption priority of each process. The availability of hardware and software, current backup files, telecommunications, and the reload time requirements of the host platform dictate the specific time frames for recovery. The minimum time-frame expected to restore any computer system or application to status and fully operational is “24” to “72” hours following the installation, checkout, and turn-over of backup or replacement platforms.

13. Recovery Goals: All DFAS personnel must understand that following, a major interruption of the Agency’s services

and operations, **is not a matter of “business as usual” - it is a matter of “survival”!!!!**

E. PREVENTION. A major objective of contingency planning is to avoid or lessen the impact on operations of an adverse situation. Therefore, the COOP plan must include measures or actions to protect DFAS assets and manage risk to prevent an adverse action from becoming a disaster situation from which DFAS may not recover.

1. Risk Assessment or Business Impact Analysis.

a. General. Perform a risk assessment (RA) or Business Impact Analysis (BIA) to identify the expected vulnerabilities based on estimated probabilities of the occurrence of certain events. In addition, the BIA assesses the projected impact on operations evaluated in specific monetary terms for worst case losses. This information becomes the foundation for developing programs to reduce the impact of a threat and identify resource requirements to solve specific risk associated problems. Update the RA or BIA annually to determine adequacy of recovery strategies, validate critical time frames, dependencies, and identify needed preventive actions.

b. Possible Threats to DFAS Activities. DFAS activities and DFAS service providers are vulnerable to a wide range of threats due to the location of our facilities. Recent natural disasters such as hurricanes, tornadoes, earthquakes, flooding, etc., have caused death, destruction and resulted in large monetary losses in geographic areas that are in close proximity to DFAS sites. In today’s environment, natural as well as other threats involving modern technology are reasons for concern. The following is a list of possible threats that have the potential for causing harm and impairment to our facilities and people:

(1) Natural Threats. The damage resulting from natural threats can range from minimal to major. The impact can have a long-term effect on the infrastructure at any given location. Threats in this category include:

(a) Avalanche,
(b) Dam failure,
(c) Tornado,
(d) Earthquake,
(e) Flood,
(f) Hurricanes or tropical storms,
(g) Landslide,

(h) Volcano,
(i) Wildfire, and
(j) Winter storms (ice and snow).

(2) Technological (Man-made) Threats. Advances in modern technology have dramatically expanded this category of threats. These threats are frequently unpredictable; can affect localized or widespread areas, cause substantial loss of life and damage to property, and pose a significant threat to the infrastructure. Technological threats include:

(a) Hazardous materials or radiological,
(b) Power failures,
(c) Information attacks (i.e., Computer viruses, etc.),
(d) Structural fires,
(e) Transportation accidents of all types,
(f) Airborne poison or chemicals,
(g) Water supply contamination
(h) Bombs or explosives, including car bomb,
(i) Armed employee or intruder, and
(j) Work stoppage/furlough.

(3) National Security Threats. These types of threats come from hostile forces to the land, population or infrastructure of the United States. Similar to other categories, national security threats are either predictable or unpredictable, and include:

(a) Nuclear attack,
(b) Chemical and biological warfare,
(c) Terrorism,
(d) Subversion,
(e) Insurgency, and
(f) Drug trafficking

2. Emergency Evacuation and Response COOP Plans. These plans should identify key points of contact and responsibilities for building management, police services, bomb disposal, hazardous material, utilities, medical, and government emergency support agencies such as the General Services Administration (GSA) and local or state Emergency Management Agencies. Specify key DFAS personnel and their crisis response team (CRT) or crisis evacuation team (CET) duties. Describe the emergency reporting or management structure and the management decision process and involvement in declaring and responding to an emergency.

a. Evacuation COOP Plans. The Emergency Evacuation COOP plan should contain procedures for the orderly evacuation of the building including responsibilities of CET and CRT personnel, assembly control points, and accountability of personnel. The plan should also address alternate evacuation procedures.

b. Crisis Action Packages (CAPs). Develop CAPs for each type of threat that poses a significant risk based upon the Risk Assessment (RA) or Business Impact Analysis (BIA). For example, if the site is in a hurricane zone develop a CAP identifying actions needed to prepare for a hurricane including, briefing of personnel evacuating out of the area, securing the building, and cleanup procedures, etc. The CAPs should also include pre-written correspondence for quick release in an emergency. For example, a notification letter activating a contingency contract. (Instructions on CAP development are at Appendix B.)

c. Contingency Contracts or Agreements. Negotiate contingency contracts or agreements in advance to provide for expedient or continuous service in case of a contingency situation. The type of contingency contracts or agreements needed will vary by location, but should include the following common areas:

(1) Agreement with facilities provider (usually GSA) to find local, suitable replacement facilities within a specified time, usually 1 week for temporary and 90 days for semi-permanent or permanent.

(2) Emergency purchase or repair of equipment, commercial off-the-shelf (COTS) software, supplies, etc.

(3) Emergency transportation or travel arrangements for transporting personnel or physical resources.

(4) Emergency alternate utilities such as power generators, water coolers, portable heaters, and portable toilets, etc.

(5) Un-interruptible power supply to provide for emergency power and controlled shutdown of operations to protect critical or sensitive automated equipment and software.

(6) Redundant communication lines and other emergency communications capability such as a contingency data line (T1) to provide for emergency telecommunications.

(7) Emergency cleanup or facility restoration such as water extraction and removal.

(8) AIS backup processing and off-site storage of files.

(9) Storage of special equipment or supply requirements off-site or at the alternate or backup site.

d. Special Emergency Equipment. Keep equipment needed to respond to an emergency on-hand or at an alternate site for quick retrieval. Key emergency personnel should possess walkie-talkies or cellular phones to coordinate the emergency response or evacuation effort. Equip the CCC with secure phones, secure FAX, secure PC, television, radio, flashlights, first-aid kit, etc.

F. COOP PLAN CONSTRUCTION USING LDRPS. The COOP plans in LDRPS should provide information needed to respond and recover from a disaster. This includes where to go (**locations**), what people to notify for response or relocation (**teams and employees**), what to do (**tasks**), who to report to (**reporting structure**), who else to notify (**customers**), where to obtain needed support (**service providers**), critical resources needed (**automated equipment, software, telecommunications, assets, vital records and supplies**), in order to provide for continuity of operations of business functions (**processes**). The LDRPS Users Guide and Training Guide contain detailed information regarding COOP plan construction. The following provides general guidance on contingency information captured in LDRPS.

1. Sensitive Information in LDRPS. LDRPS may contain sensitive information such as the Agencies backup arrangements as well as information subject to the Privacy Act. **Do not store classified information in the LDRPS database**. Reference classified documentation in LDRPS and store in an approved security container. Identify all LDRPS generated reports “For Official Use Only”. Reports containing Privacy Act information should include a statement advising of the authorized use of the information in accordance with Executive Order 9397 and Section 6311 of Title 5 to the U.S. Code. Identify LDRPS data fields containing information subject to the Privacy Act with a Privacy Act statement authorizing collection of this information.

2. Personnel.

a. Successors (Contingency Reporting Structure).

(1) Chain of Command Succession. Each organization's COOP plan must specify successors, alternates to replace Agency authorities, key personnel, and the order of succession and conditions under which succession and termination will occur.

(2) Chain of Command Succession -- DFAS-Headquarters. No person within this Agency is slated to succeed a person outside this organization (DoD Directive 3020.4). Within the Agency, however, if the DFAS Director dies, is disabled, or is absent, the incumbents in the DFAS-Headquarters positions listed as follows shall succeed to the position of, and act as, Director, Defense Finance and Accounting Service:

(a) Principal Deputy Director

(b) Deputy Director for Finance

(c) Deputy Director for Accounting

(d) Senior Executive Service (SES) Officer Deputy Director based on the following precedence: first in order of Executive Service pay rate, date of rank, then seniority in Agency.

(3) DFAS-Headquarters Chain of Command Succession by Center Director. In the event of death, disability, or if one of the Headquarters SES Deputy Directors is not available, the senior Center Director shall succeed to the position of, and act as, Director, Defense Finance and Accounting Service.

b. Key or Critical Personnel. Designate primary and alternate staff personnel or positions including service providers needed to perform essential functions during an emergency response, or at the recovery (alternate or backup) and/or reconstitution relocation sites. Such personnel shall include:

(1) Emergency Staff Designees. Individuals who, on short notice, can move to designated control site or emergency relocation sites, form an emergency staff or augment an existing command element, and perform essential functions. Create small emergency staffs capable of performing their offices' essential functions.

(2) Alternate Command Personnel. Minimal staffs at alternate command centers ensure continuity of

essential functions during an emergency and serve as the nuclei for relocated emergency staff. Assign these personnel permanently or on a rotational basis to emergency facilities. These personnel will:

(a) Maintain a minimal alternate command center capability.

(b) Perform designated essential functions when their primary command post or center is inoperable, destroyed, or as directed.

(c) Support the primary command center and integrate into the emergency staff when it operates from the home site, or serve as the core for the reconstitution of damaged or destroyed headquarters.

(3) Skills. In determining the number of essential personnel, consider using people with multiple skills to reduce the number of people required. Also, designated key personnel should not include members of the Selected Reserve (drilling Reservists or National Guard), or military pre-trained personnel (Ready Reserve or military retirees) subject to military recall or mobilization.

(4) Emergency Staff (key personnel). Identify the number and distribution of emergency staff positions in the COOP plan. Key personnel shall participate in periodic exercise testing of emergency procedures.

c. Accountability. Recent catastrophic contingency situations, such as terrorist bombings, have accentuated the need to account for all employees. Provide a means to easily locate and validate employee presence.

d. Notification. The COOP plan should provide for individual notification of employees as well as the emergency points of contact. Cover the following type of information so the person responsible for notification knows:

(1) Who is to contact who and in what priority?

(a) Appropriate actions for contacting employees especially after normal business hours.

(b) Advise employees regarding what they are to do, what is expected of them, and where they are to report.

(c) Special leave or furlough considerations.

(2) In case of employee injury or fatality, who has responsibility to notify the emergency point of contact and how are they are contacted.

(3) When and how to contact customers and service providers and in what order.

e. Trauma Counseling. The COOP plan should provide for the needs of employees directly involved in a contingency situation. This includes designating responsibility for monitoring employees for symptoms of exhaustion or post-traumatic stress disorder (PTSD) and providing trauma counseling to victims.

3. Teams and Tasks. This COOP plan construction category is the most important part of the LDRPS "dynamic" plan. Tasks are the step by step procedures performed by the various teams in an emergency response or recovery situation. Detail the tasks in a manner that someone not familiar with a business process or function can recover operations. Depending on how static the organization is, assign employees to the various positions. Assign an employee as a team leader for all applicable teams. The following are examples of general emergency teams and tasks:

a. Emergency (Crisis) Management Team (EMT or CMT).

(1) Responsibility: Coordinate all casualty control decisions and implement recovery operations. This team responds to the information provided by the Crisis Response Team (CRT) and the Crisis Coordination Team (CCT).

(2) Membership: Director and/or Principle Deputy Director of the DFAS entity, Director of each Directorate or Deputate as needed, and Public Affairs Officer.

(3) Assembly Location: Normally assemble at the Crisis Coordination Center (CCC). Personnel assigned to the CMT should have a SECRET clearance, including a statement in their position description, since they may need to handle classified information as part of the normal conduct of contingency coordination in the CCC.

b. Emergency (Crisis) Coordination Team (ECT or CCT).

(1) Responsibility: Coordinate the response and recovery efforts. The CCT should record significant events as they occur and the impact of the event.

(2) Membership: Normally consists of the Director of Plans and Management and Contingency Planning Working Group (CPWG) members who are normally working level representatives from each Directorate or Division or major functional area.

(3) Assembly Location: Assembly area is the CCC or alternate CCC. Personnel assigned to the CCT should have a SECRET clearance since they may need to handle classified information.

(4) Actions:

(a) Keep the CMT apprised of the efforts of the other teams and distribute and control taskings levied by the CMT.

(b) Provide assistance to the Crisis Response Team (CRT) and notifying other teams of the status of response and recovery efforts. The CCT should notify appropriate emergency action teams and initiate recovery operations.

(c) Determine feasible approaches for recovering vital functions and recommend recovery procedures and priorities to the CMT based on the assessment of damages and capabilities.

(d) Reports the emergency to other DFAS organizations including DFAS-Headquarters using the SITREP procedures described in Appendix A.

c. Emergency (Crisis) Response Team (ERT or CRT)

(1) Responsibility: The CRT is responsible for on-site assessment and evaluation.

(2) Membership: Membership normally consists of the Deputy Director of Resource Management (as the CRT leader); Chief of the Facilities Branch or Division, Building Security Officer, Information Security Officer, Public Affairs Officer, Safety Officer, Automated Information Systems representative, and representative(s) from the affected area(s).

(3) Assembly Location: Normally the CRT will assemble at the scene of the crisis, or at another predetermined location.

(4) Actions:

(a) Reports the casualty and damage situation to the CCT.

(b) The team leader confirms the emergency, officially declares the disaster, orders an immediate evacuation if the situation is life threatening and notifies the CCT of the emergency and the general location.

(c) Provides the CCT with a timely assessment, evaluation, and notice of escalation regarding the emergency. Based on the assessment of the emergency, the CRT should recommend actions needed for the recovery effort to the CCT.

(d) Upon arrival, civil police or fire personnel will assume control of the incident until the emergency situation is resolved. The CRT reports and provides information through the Civil Incident Commander until the scene is returned to the control of DFAS.

d. Emergency (Crisis) Evacuation Teams (EET or CET).

(1) Responsibility: Ensure the safe evacuation of DFAS facilities.

(2) Membership: Pre-designate emergency personnel as building fire marshals, floor wardens, area monitors, elevator and stair monitors, safety officers, and facilities’ representative, as appropriate to control and assist with the evacuation. Assign special wardens to ensure handicapped or mobility impaired personnel receive needed assistance.

(3) Assembly Location: Predetermined locations.

(4) Actions: Document the duties of the CET in the Building Evacuation Plan.

e. Emergency (Crisis) Recovery Action Teams (ERAT or CRAT).

(1) Responsibility: Responsible for actions necessary to recover time sensitive operations based on critical time frames and the acceptable number of days delay.

(2) Membership: Each major process or function should have a CRAT composed of appropriate membership from the organization necessary to recover operations.

(3) Assembly Location: Predetermined in plan.

(4) Actions:

(a) Determine requirement to relocate to a backup or alternate site as well as incorporate alternate recovery strategies such as manual procedures and recovery of backup documentation from off-site storage or from the originator.

(b) Responsible for recovery efforts for the process or functions up to the point of full reconstitution to normal operations.

(c) The CRAT leader is responsible for implementing appropriate recovery actions including notification and guidance of personnel needed to support the recovery effort.

f. Emergency (Crisis) Support Teams (EST or CST).

(1) Responsibility: Provide support for the recovery effort.

(2) Membership: May include Emergency Telecommunication (ELAN) Team, Emergency Logistic Team, Emergency Transportation Team, Emergency Administrative Support Team, or Emergency Security Team.

(3) Assembly Location: The assembly area will vary depending on the crisis and the type of support provided.

(4) Actions: Arrange for emergency transportation of personnel and physical resources, emergency procurement, emergency reproduction, emergency retrieval of vital records from off-site storage, etc.

g. Automated Information Management System (AIS) Recovery Team (ART).

(1) Responsibility: Assist with the recovery efforts of the AIS service provider, such as the DISA Mega Center.

(2) Membership: All critical AISs should have an ART composed of representatives from the functional and FSA areas who possess technical knowledge needed to validate the recovery.

(3) Assembly Location: Predetermined in the plan. The ART may need to temporarily relocate to the service provider's backup processing site.

(4) Actions: Ensure AIS recovery efforts are expedient and proper. Key personnel designated to provide support for recovery of critical AISs at the DISA back-up site should have a SECRET clearance to ensure access to the DISA facility.

4. Functions and Processes.

(1) Major (Critical or Essential) Business Functions. Essential business functions are core or vital functions accomplished regardless of the emergency circumstances to fulfill assigned mission(s). Within DFAS, essential functions consist of processes that are time sensitive and critical to accomplishing the DFAS mission. Mission essential functions include: military pay, civilian pay, retiree pay and annuities, travel pay, transportation pay, vendor pay, contract pay, and security assistance and foreign military sales. Other functionssuch as human resources (personnel), resource management and the FSO/FSAs should provide support for the core or essential functions.

(2) Processes. A major business function may have one or more critical or time-sensitive processes. In addition, during a local crisis or national emergency, it is possible to curtail, de-emphasize or eliminate some processes. Examples are creating non-essential reports, or terminating the development of new, non-critical applications. Depending upon the situation or crisis, other processes may receive greater emphasis, and new processes may become necessary. These processes may include immediate payment of additional personnel, ad-hoc work around solutions, urgent status reports to higher headquarters, or developing new programs for the payment of new or increased entitlements to military personnel.

(a) Criticality Designation. Rate the criticality of a specific process in the COOP plan as (M)ission, (D)irect support, or (I)ndirect support. The priority of the process is scenario dependent and can change during the time of month or year. Delineate the essential processes in each organization's COOP. This includes indicating during what periods of the month the function is critical and the allowable number of days delay.

(b) Resumption Priority. Identify the priority for recovery of a process within a criticality rating as 1, 2, 3, or 4, with 1 being a top priority.

(c) Employees. Identify the number of employees needed to support the short, mid, and long term recovery efforts for relocation to an alternate or backup site or for mobilization support for each process.

(d) Other Resources. If there is more than one process assigned to a COOP plan, then identify specific resources needed to support each process. This includes applicable software (AISs), supplies, equipment, telecommunication, teams, and other dependent processes.

5. Software -- Automated Information Systems (AISs).

a. AISs are an important and essential in providing services to the DoD finance and accounting community. Therefore, place special emphasis on maintaining day-to-day operations of automated information systems, and on the quick recovery of essential computer capabilities when an unplanned disruption occurs.

b. Preventive Measures. The COOP plan should include the following preventive measures to adequately prepare for continuity of operations for AIS requirements in accordance with DoD Directive 5200.28, DoD Directive 3020.26, and DFAS Regulation 8000.1.

(1) Off Site Storage. Send copies of critical application programs, system data files, and documentation, to a federally certified vaulted or underground storage site for protection. Each data processing facility should develop implementing programs and procedures that ensure compliance and inventory control of the stored items. Procedures should include an independent annual verification of compliance. The data processing facilities supporting Centers and remote activities will comply with the off-site storage and inventory requirements, delineated in support agreements.

(2) AIS Files Back-up. Back up all computer software and data files required to implement recovery of mainframe, mid-tier, wide or Enterprise Local Area Network

(ELAN) operating environments, and personal computers that support time-sensitive business operations daily or at other regularly scheduled processing times, as appropriate. Rotate backup files and retain off-site weekly or at a pre-determined period sufficient to ensure the protection of data and applications software. The business manager should approve the type of backup and the timing of the off-site rotation and ensure the strategy is sufficient to minimize the re-entry or re-construction of data and enable the recovery of files to current status.

(3) Processing Back-up. The COOP plan should include sufficient information regarding the AIS to enable emergency recovery. This includes the identification of critical AISs, the critical time frames and allowable days delay, contingency job streams, AIS dependencies, hardware requirements, supporting software requirements including contingency licensing information, critical products, points of contact, etc. The COOP plan should also identify the backup AIS processing location.

(4) Backup COOP plans for AISs supported by a Service Provider. Since DFAS operations are so dependent on AISs it is necessary to protect all critical or time sensitive automated data processing by a backup system and have COOP plans in-place for recovery. In carrying out this policy, support agreements with AIS service providers, such as DISA, should include requirements for developing and maintaining contingency plans to ensure continuity of operations for DFAS AISs that they support. The attainment of this goal depends upon equipment inter-operability and sufficient capacity to support additional requirements. This should include critical time frames and acceptable delay, requirements for hardware, software, and telecommunications backup processing support and identify the location of the backup processing support. The COOP plans should also specify the backup, off-site storage, and retrieval of software and data files as well as software licensing agreements for operating at a backup site. In all cases, AIS COOP plans must comply with DoD regulations and standards. DFAS activities shall identify backup requirements in appropriate letters of agreement, memorandums of understanding, service support agreements, or contracts.

(5) Coordinate AIS Recovery COOP plans. Closely link DISA recovery strategy with DFAS operations. Such COOP plans must include restoring data processing capability after partial or complete destruction of equipment or facilities. Depending upon the specific situation, recovery COOP plans should portray short and long-term actions such as

deferring non-essential functions, restoring existing facilities, using contractors or vendors, and obtaining stored information. In all cases, recovery COOP plans must include procedures that periodically retrieve files from off-site storage and verify the recovered information.

6. Telecommunications. Telecommunications are the back bone of DFAS operations. Therefore, it is important to minimize or, if possible, eliminate all single points of failure by installing alternate communications redundant lines and implement other preventive measures for expeditious repair and recovery of network connectivity. Since telecommunication is in most cases a cooperative effort between DFAS and DISA, it is imperative to define the responsibility for each part of the network and protect by recovery COOP plans. This includes storing on-site backups of sensitive, critical equipment, such as file servers and internal routers. In addition, document in the COOP plan specific requirements for telecommunications to enable reconstruction of the connectivity at a backup or alternate site.

7. Emergency Procedures. COOP plans shall specify emergency procedures including the identification of emergency staff assignments, emergency duty stations, notification procedures, personnel accountability requirements, and other actions to take under various emergencies. Maintain a checklist of emergency actions or tasks performed during critical periods at primary and alternate headquarters and relocation sites. Develop appropriate Crisis Action Packages (CAPs) to supplement the checklist and include point papers, briefings, and implementing documents such as pre-prepared acquisition documents.

a. Procedures in the Event of Prior Warning. Emergency team members or designees should report to assigned locations when directed by the Secretary of Defense, DFAS Director, or Center, OPLOC, FSA, or DAO Director or their designee. Use Government provided transportation, when possible. Use private transportation if necessary. As a rule, movement of essential staff personnel should begin before a known disaster occurs. Issue special instructions and special passes to emergency staff designees to facilitate movement and access to emergency and alternate duty locations. Non-emergency staff members shall comply with COOP and local civil defense instructions.

b. Procedures for Reporting.

(1) DFAS Organizations. During a catastrophe normal communications channels with parent organizations may fail. In the event communication channels with higher headquarters fail, DFAS organizations shall communicate with the nearest DoD activity in communication with the National Command Authority by any means available, giving a brief status report of activities, capabilities, requirements, and resources.

(2) DFAS Military and Civilian Personnel. DFAS personnel should report to their emergency or normal duty stations or emergency assembly or control area. If unable to reach either, they should contact the nearest surviving DoD or DFAS installation for further instructions. Some DFAS entities have toll free numbers for emergency reporting purposes.

(3) Families. Each individual with an emergency team assignment has primary responsibility to arrange for care of their families. However, it is in DoD's interest to assist emergency staff members for emergency care of family members. Supervisors should:

(a) Ensure that emergency team designees do not have extreme personal or special problems that could preclude their reporting to their emergency duty stations and carrying out their assignments.

(b) Arrange for emergency communication between relocated employees and their families, if possible.

(c) Make provisions, in coordination with local or state civil defense authorities, for the movement and care of family members in the general area of the designated emergency site.

(d) Urge emergency staff members to instruct their families on emergency actions to take in their absence.

8. Vital Records. The COOP plan should identify vital records and the backup storage information. Maintain all documents and automated data processing (ADP) software and databases required to carry out essential functions, particularly during and immediately following a disaster, in emergency files available to alternate or backup relocation sites. The DFAS-Headquarters, Centers, FSO/FSA, and OPLOCs are responsible for establishing the content and the procedures for updating the information in its emergency files. The organization's COOP shall contain instructions for the preservation of vital documents, records, and files. DFAS

Records Management Program, DFAS 5015.2-R, contains specific responsibilities and requirements regarding vital records.

9. Locations (Control Site, Relocation Sites, and Off-site Storage Locations). The COOP plan should identify control sites including emergency assembly areas, alternate (local) recovery sites, backup (non-local) recovery sites, and off-site storage locations for storing vital records including automated files. Logistics, economics and timeliness are among the deciding factors regarding possible locations. Make arrangements to use Government facilities/capabilities to the maximum extent possible. This includes agreements with National Guard and Reserve Armories for transportation and accommodations. The COOP plan should include directions, information regarding transportation of personnel and resources, the point of contact at the location, and the supplies and services available at the location.

a. Control Sites. Establish control sites for crisis coordination and management, an alternate coordination and management location, building evacuation assembly area, and emergency assembly or reporting area for key personnel. Where feasible, obtain agreements to use the resources and facilities of the local State or Federal Emergency Management Agency (SEMA or FEMA) for a command center if local DFAS facilities are not usable.

b. Alternate or Backup Emergency Relocation Sites.

(1) An alternate or backup headquarters is a fixed or mobile headquarters or subordinate command designated to assume the responsibilities and functions of the primary headquarters under prescribed emergency conditions.

(2) An emergency alternate or backup relocation site may receive all or portions of the organization’s critical operations. It may be inactive or staffed on a standby basis to maintain the facility, communications, and databases. The relocation site should be able to activate rapidly, support the initial requirements of the relocated elements for a predetermined period, and expand to meet restoration requirements.

(3) Alternate and backup emergency sites should be outside prime target areas or areas especially vulnerable to technological or natural disasters.

c. Off site Storage Locations. Store backups of vital records and critical supplies, equipment, and other assets at a location outside the immediate geographic area.

The off-site storage area should be outside the same regional disaster affecting the on-site location.

d. Reconstitution Location. Each COOP plan should include reconstitution procedures for reestablishing the required facilities through rehabilitation or by requisition of other suitable, available facilities. In most cases, the General Services Administration has the responsibility for obtaining these replacement facilities based on written agreement with the DFAS entity.

10. Assets, Automated Equipment, And Supplies. The COOP plan should identify resource requirements for short, mid, and long-term recovery at an alternate or backup site. This includes assets such as work stations and chairs, equipment such as personal computers, and supplies such as paper and forms. Store resources needed for resumption and recovery off-site for easy and quick use or created from other identified sources. Store on site backup files in a fire resistant safe or in a location that is remote from the business and technology operations area. Locate backup resources off-site outside the immediate geographic area and in an area not affected by the same regional disaster affecting the originating location.

11. Public Affairs Officer. Identify in the COOP plan designated persons to provide information to the news media in case of an emergency. Providing the news media with early, factual and consistent information is very important to help ensure accurate and unbiased reporting as well as fostering public support. News releases are effective to broadcast emergency information for employees.

12. Transportation or Emergency Travel Funds Authority. Identify persons assigned to provide travel authorization, approve advance payments, make travel arrangements, and arrange transport of personnel, supplies, vital records, equipment, backup files, etc.

13. Emergency Procurement. Identify authorized emergency procurement authority and authorized emergency funds limit.

G. SECURITY AND MAINTENANCE OF THE LDRPS DATABASE.

1. Security. Maintaining the integrity of the sensitive data in LDRPS is essential. Passwords control user access to LDRPS. In addition, built-in security allows controlling and limiting access to specific screens, data fields, and reports in LDRPS.

2. Audit History. LDRPS creates an audit history of all transactions. This history can be helpful in determining LDRPS activity, identifying problems, as well as assisting with recovery of LDRPS.

3. LDRPS maintenance and backup.

a. Routine. The LDRPS systems administrator (contingency planning staff or other delegated Center/FSA personnel) shall perform routine maintenance weekly or as needed. Routine maintenance includes printing and purging the audit history file (print to electronic media rather than paper), reconstructing the database, and backing up the LDRPS data and text files.

b. Backup. Backup the LDRPS database and software according to normal Enterprise Local Area Network (ELAN) backup operations. Normally accomplish a full backup weekly with daily backup of transactions. Store the full backup off-site with other critical ELAN backup files. Load the Disaster Recover Plan (DRP) backup accomplished by the LDRPS systems administrator on the CCC backup notebook PC. Maintain this notebook off-site, away from the LDRPS host application server.

4. Changes to LDRPS.

a. Locally Authorized Changes. The local LDRPS system administrator can make routine changes to LDRPS such as user security access, pick lists, help bar, or required fields.

b. DFAS-Wide Changes. DFAS-HQ/M must approve any changes to add or modify data fields or standard DFAS reports.

c. Custom Reports. The local LDRPS systems administrator can develop unique custom LDRPS reports using LDRPS. Submit reports useful by other DFAS entities to DFAS-HQ/M for distribution DFAS-wide.

d. Change Control. Changes to the standard LDRPS configuration may result from the need to add a new field, change the field size or name, new DFAS report, new DFAS-wide security group, etc. The DFAS-Headquarters Director of Plans and Management or designee must approve any changes, additions, or deletions to the LDRPS data fields or standard reports or security groups. All changes receive a change control number. DFAS-HQ will monitor the changes to ensure standard application of LDRPS DFAS-wide. The Center/FSA contingency planners designated as LDRPS systems administrators can change or add pick-lists, filters, entity unique custom reports as needed without prior approval of DFAS-Headquarters.

H. COOP PLAN ACTIVATION.

1. Authorized Official. The Secretary of Defense, DFAS-Headquarters, Center, OPLOC, FSO, FSA, or DAO Director or their designee activates the COOP plan.

2. Activation of LDRPS Backup Copy. Under a separate agreement, Strohl Systems, Inc. authorized maintenance of backup copies of LDRPS by the DFAS-Headquarters, FSO, FSA, and OPLOCs. **WARNING**: Use of these copies requires activation of a contingent contract. To activate one of these backup copies requires notification of DFAS-HQ/M who in-turn must activate the contingency contract to buy an additional copy of LDRPS at approximately $25,000.

I. COOP TESTING AND EXERCISES. There are three types of COOP tests or exercises in addition to the mobilization exercises discussed in Chapter 4: (1) paper test involves reviewing hardcopy information including reports from LDRPS, (2) table top test is an in-place review and open discussion of COOP plans by a group or committee based upon a specific scenario, and
(3) live test of the COOP plan under simulated emergency conditions requiring relocation to an alternate or backup site. **Conduct a table top test prior to a live test to maximize results and minimize cost.**

1. Testing AISs. Data processing operations are, historically, volatile in nature. This occurs because of frequent changes to equipment, programs, documents, customer service, and daily operational changes. The application systems program manager and office of responsibility shall design backup programs and procedures for the operation of each AIS to ensure continuity of operations for all corporate systems.

a. Newly Developed AISs. The AIS project manager or officer must test and demonstrate an executable COOP plan before deploying the system.

b. Existing AISs. After implementation, review and certify backup application programs and stored files for accuracy and currency at least annually or when a change is made that affects the AIS. Test critical AISs “live” at the backup facility environment at least every three years. Testing should include telecommunications as applicable for recovery and operation of the AIS. Test any automated interfaces with the AISs required for processing. Jointly test recovery of an AIS embedded or integrated into another system for which DFAS does not have primary responsibility.

c. Scheduling AIS Tests at DISA backup facilities. Tests of AISs at DISA backup facilities are scheduled annually by DISA. Centers will submit requests to schedule test of DFAS AISs at DISA backup facilities to DFAS-Headquarters NLT than May 1 of each year. DFAS-Headquarters will coordinate with DISA to include the requested test in the schedule for the next fiscal year.

2. Non-AIS Exercises. Non-AIS exercises include testing procedures for the emergency evacuation of facilities, emergency notification of employees during non-duty hours, or relocation to an alternate or backup facility. Each DFAS entity should conduct at least one non-AIS exercise each quarter. **CONDUCT AT LEAST ONE LIVE NON-AIS EXERCISE ANNUALLY.**

3. Test or Exercise COOP plan. Develop an exercise Plan for each test or exercise. The amount of information required in the Plan will vary by the type of test or exercise and the scope. As a minimum, each test plan should include a brief scenario description, type of test, scope of the test, and participants in the test and their responsibilities. Tests involving AISs should be a joint effort of the business operations manager, the FSA or other Central Design Activity, and the data processing service provider to develop detailed test plan. The test Plans delineate resource requirements such as hardware, software, data files, and desired inputs/outputs. The Center Contingency Planning Office should request a point of contact at each DISA Defense Mega Center (DMC) to coordinate, monitor, and initiate the data processing test and evaluation plans.

4. Test or Exercise Evaluation Report. Document problems encountered and lessons learned in an Evaluation Report. Submit this evaluation report to the Center, FSA, or OPLOC Director and the DFAS-HQ/M within 30 days of completion of the test or exercise. Document any open issues not resolved during the test or exercise and track until resolved.

CHAPTER 4

SUPPORT TO CONTINGENCY OPERATIONS AND MOBILIZATION

A. GENERAL.

1. Since activation in January 1991, the Defense Finance and Accounting Service has assumed a much larger role in supporting the Combatant Commanders and the Services during contingency operations than was originally envisioned by the Agency. DFAS provides direct support to deployed tactical finance forces and has a key role in developing the finance policies and systems necessary to complement this support.

2. This chapter addresses the DFAS role in support of contingency operations and mobilization by describing the assistance DFAS will provide to meet the needs of the Services. It also includes broad policy guidance and identifies actions required to provide support during a contingency operation and mobilization.

B. DEFENSE FINANCE AND ACCOUNTING SUPPORT ELEMENT (DFASE).

1. General. DFAS does not have tactical units to deploy in support of the Combatant Commanders. However, as the Principal DoD Executive Agent (DoDD 5118.5) for finance and accounting requirements, systems, and functions DFAS has an essential role in supporting the Joint Staff and the Combatant Commanders. DFAS support consists of: a) assisting with the development of financial management plans, policies, and procedures; b) providing a single point of contact on financial matters for the Combatant Commanders and the Joint Staff; and 3) The full integration of the agency Crisis Management System (CMS) into the DoD Crisis Management System to coordinate support if there is a crisis or contingency operation. To accomplish these functions DFAS formed a Defense Finance And Accounting Support Element (DFASE) to coordinate support to the Joint Staff and the Combatant Commanders.

2. Defense Finance and Accounting Support Element (DFASE) Roles and Missions.

a. DFASE is the focal point for joint financial management initiatives and issues for the Joint Staff (J-8) and the Commander-in-Chief (CINC) Comptrollers. In this role, members of the DFASE meet with and routinely communicate with the CINCs staff and the J-8 in peacetime. DFASE assists with the development of financial management annexes to theater contingency plans, Standing Operating Procedures (SOP) for the staff, and developing training scenarios for the CINCs staff and JCS exercises.

b. DFASE consists of representatives of each of the DFAS-Headquarters Deputy Directors, Centers and the FSO. The Director, Planning and Management Support Directorate (DFAS-HQ/MP) is the Director of the DFASE.

c. As a deployment becomes imminent, the interaction between DFASE, the Joint Staff and the Warfighting CINC increases substantially. The DFASE:

(1) Provides the Warfighting CINC a single point of contact for all issues related to financial support in the theater. This ensures the CINC/JTF Commander/Executive Agent has the critical information to make informed decisions early in the deployment. In addition, DFAS coordinates with the DFAS activities to prepare them to provide the support required by deployed forces.

(2) Convenes DoD working groups to make timely decisions on joint polices and procedures on entitlements for deploying forces. These groups will meet before the deployment execution order and consists of representatives from the Services, the Joint Staff, Under Secretary of Defense (Personnel and Readiness, Per Diem, Travel, Transportation Committee and Compensation Committee).

(3) Develops responses to probable contingency operations issues in advance of the operation to permit the timely response with accurate and timely recommendations in support of deploying forces.

(4) Provides, on request, liaison personnel to support the CINCs or the Joint Task Force Commander. This individual(s) will assist in development of finance policy and coordinate DFAS finance support for deployed forces.

C. CRISIS MANAGEMENT SYSTEM SUPPORT OF CONTINGENCY OPERATIONS AND MOBILIZATION.

1. OSD Crisis Management System (CMS). DFAS is an active participant in the OSD CMS. DFAS personnel routinely review world wide messages sent to the Joint Staff on finance and accounting issues raised by theater commanders related to daily military operations. If there is a deployment, DFAS personnel will permanently locate to the OSD Executive Support Center to quickly respond to Joint Staff requirements for financial support. Active participation in meetings and discussions by the Joint Staff is critical in order to provide timely support to the deployed forces.

2. DFAS Crisis Management System (CMS). During the early stages of a national crisis or contingency operation the DFAS Director may activate the DFAS CMS. Activation of the CMS will

result in the HQ Crisis Coordination Center (CCC) and the CCCs at the five Centers and appropriate OPLOCs initiating round the clock operations to rapidly disseminate information on the crisis/operation and coordinate support for deployed forces.

a. The DFAS CMS provides the secure systems to communicate with the CINCs staff, deployed Commander, designated Executive Agents for support, and the DFAS providers of support.

b. Activation of the DFAS CMS will also activate Crisis Action Teams made up of functional experts to enable prompt response to policy issues or support requirements.

D. CONTINGENCY OPERATIONS PLANNING SCENARIOS.

1. Two Major Regional Conflicts. The execution of two nearly simultaneous MRCs will have a dramatic impact on DFAS operations. DFAS Centers, OPLOCs and installation level support offices will experience a dramatic increase in workload. DFAS may also lose large numbers of employees due to reserve activation. The parent service might also recall military personnel assigned to DFAS, requiring a backfill of personnel for continuing support. Manpower requirements might result in retirees being recalled to active duty. DFAS Centers, OPLOCs and installation level support offices must plan to absorb the increased workload and provide personnel to replace those personnel lost.

2. One Major Regional Conflict. Supporting a single MRC will have a significant impact on operations. Workload will increase at many DFAS Centers, OPLOCs and installation finance organizations. Large numbers of active duty finance personnel may deploy, possibly requiring a backfill of personnel to provide continuing support at some installations. Reservists in DFAS organizations are also subject to activation. Retirees are unlikely to be involuntarily recalled, but some may voluntarily return to active duty. While the impact of a one MRC is less than a two MRC operation, DFAS Centers, OPLOCs and installation level support offices must plan to absorb increased workload and replace any personnel lost due to mobilizations or deployments.

3. Major Deployment, Primarily CONUS Units. A deployment consisting primarily of CONUS units could have a significant impact on some installations. The departure of active duty finance units from CONUS installations could result in the deployment of most of the finance support at the installation. This might necessitate DFAS providing a backfill of personnel at those installations. Some recall of reservists may occur which could affect DFAS operations at some activities.

4. Major Deployment, Primarily OCONUS Units. A deployment consisting of primarily OCONUS units will have minor impact on DFAS. We can anticipate a surge in workload requirements at the

Centers to support the deployment. Mobilization requirements might affect installation level operations. The Army, in particular, during recent operations has activated a centralized processing site for reservists activated to support the deployment. Expect a surge at the beginning of the deployment and another surge at the end of the operation. Activation of reservists assigned to DFAS organizations as civilian employees might affect some DFAS operations.

5. Small Deployment, Primarily CONUS Units. A deployment consisting of primarily CONUS units will have minimal impact on DFAS. Anticipate a minor increase in workload requirements at the Centers to support the deployment. Deploying active duty finance personnel might also affect some installation level operations. Some installations might also experience a significant increase in the number of pay transactions for reservists activating to support the deployment. Expect a slight surge at the beginning of the deployment and another surge at the end of the operation. Activating reservists assigned to DFAS organizations as civilian employees might have an impact on some DFAS operations.

6. Small Deployment, Primarily OCONUS Units. A deployment consisting of primarily OCONUS units should have the least impact on DFAS. We can anticipate a minor increase in workload requirements at the Centers to support the deployment. Some installations might have a significant increase in support requirements to process activating reservists to support the deployment. Expect a slight surge at the beginning of the deployment and another surge at the end of the operation. Activating reservists assigned to DFAS organizations as civilian employees might impact some DFAS operations.

E. FINANCE BATTLEFIELD SYSTEMS.

1. One of the major lessons learned from Operation Desert Shield/Desert Storm was the need to develop deployable systems for use by tactical finance personnel. At the time, the services had “ peacetime” finance and accounting systems to support installation level operations. These finance systems were not easily portable and heavily dependent on the availability of reliable communication support. Most deploying tactical finance forces operated manually and retrograded documents to supporting finance operations outside the theater of operations.

2. DFAS is responsible for development of the software to support the battlefield systems and necessary interfaces. The Components are responsible for fielding the necessary hardware to support deployed forces. A close working relationship between the Components and DFAS is critical to ensure the systems will provide the support on the battlefield and interface with DFAS systems.

F. MOBILIZATION SUPPORT REQUIREMENTS.

1. Mobilization is the process of preparing for war or other emergencies by assembling and organizing personnel and materiel in support of the military forces. In preparing the forces, the U.S. Government could activate or federalize the Reserve Components, extend or modify service members' terms of service, expand or surge the industrial base, and place the U.S. Armed Forces on readiness alert.

2. Although the execution of mobilization plans will generally mean business as usual for most people within DFAS, the preparation, build-up, and deployment of the forces could dramatically increase the finance and accounting functions.

3. DFAS is not staffed to support the surge in workload resulting from a mobilization. This could result in a significant expansion of the work force and the need for additional staffing. The Agency must work very closely with the Components to identify support requirements and develop plans to support mobilization.

G. DFAS PERSONNEL.

1. Support of a contingency operation or a mobilization will likely have a significant impact on DFAS operations. The agency may loose personnel to support the actual operation and these operations will significantly increase the workload of DFAS organizations.

2. Military Personnel.

a. Active Duty Personnel.

(1) The active duty personnel assigned to the DFAS-Headquarters, Centers, and field activities must prepare to return to their parent service and deploy, in support of the Military Services', operational commitments, crisis, or any emergency activities. Although the support of a crisis will not require the reassignment of most Agency military personnel, all service members are available and ready to deploy if there is the requirement to expand the active force, or ready to fill an unfilled billet within a deploying unit. In some cases, special finance and accounting or other teams involving military specialists within the Agency may deploy and support the forces. These teams could deploy for the duration of a crisis or in the assistance of a short term requirement. To ensure that the military personnel assigned to the Agency are ready for all possible deployment scenarios, service members shall comply with their Service's deployment/mobilization guidance and instructions.

(2) MOA with Services. DFAS-Headquarters will negotiate and sign MOAs with each of the Services that address the status of military personnel assigned to DFAS if there is mobilization or a contingency operation.

(3) Key Positions. DFAS-Headquarters may designate, in coordination with the Services, certain essential military billets as key positions. The purpose of designating some billets as key positions is to fill certain positions with military personnel even if there is a major contingency operation. DFAS-Headquarters, Deputy Director for Human Resources, shall provide guidance on determining which positions are key positions. DFAS-Headquarters, Deputy Director for Resource Management, shall identify these key positions on the DFAS manning documents.

b. Reserve Component Personnel Working in DFAS Civilian Billets. According to DoD Directive 1200.7, the Agency will annually evaluate all DFAS civilians who are members of the Ready Reserve and the Individual Mobilization Augmentees (IMAs) assigned to DFAS to ensure they can fulfill their military mobilization assignments. Members of the Ready Reserve may not fill key billets within DFAS. Likewise, IMAs assigned to DFAS shall not fill a key position in their civilian company/organization (DoDD 1235.11). All reservists must prepare to mobilize immediately when called and consider those that cannot meet this criteria for removal from the Ready Reserve. The DFAS-Headquarters Deputy Director for Resource Management shall identify the designated key positions on the DFAS manning documents. The DFAS-Headquarters Deputy Director for Human Resources shall provide guidance on determining key positions and screening reservists within the agency in compliance with DoD Directive 1200.7.

c. Military Retirees.

(1) Military retirees are a pre-trained individual manpower asset available to expand the military force. They are subject to recall to active duty, as required, to fill personnel shortfalls due to mobilization or other emergencies. Also, they are available to release active duty military members for deployment overseas.

(2) According to DoD Directive 1352.1, the Agency will identify military and federal civilian wartime positions that military retirees can fill. The DFAS-Headquarters Deputy Director for Human Resources shall provide guidance on determining the positions suitable for assignment of military retiree and comply with the other provisions of this DoD Directive. The DFAS-Headquarters Deputy Director for Resource Management shall identify the designated positions on DFAS manning documents.

(3) A number of military retirees are civilian employees within DFAS. These people are subject to recall and should understand their Service requirements for keeping the appropriate Service informed of their civilian employment. Further, the DFAS-Headquarters Deputy Director for Human Resources shall determine if any retirees are filling key civilian billets and screen these individuals from military service.

d. Center/OPLOC Surge Support Requirements.

(1) Reserve Personnel.

(a) Individual Mobilization Augmentees. The services individual mobilization Augmentee programs provide a ready pool of reserve military personnel to meet the surge requirements of an organization. An IMA is able to train once a year with the organization, therefore, if there is a mobilization there will be a trained person familiar with the organization and procedures. The services administer the IMA programs.

(b) Reserve Units. In some cases, Reserve Units might be available to provide additional personnel to meet the surge requirements of an organization. Columbus and Cleveland Centers have reserve units which meet this requirement.

(2) Civilian Employees.

(a) According to DoD Directive 1400.31, the Agency will develop, maintain, and exercise DoD policy guidance, emergency plans and procedures, standby emergency implementing documents, organizational, and staffing arrangements required for rapidly mobilizing, expanding, and managing the Agency’s civilian work force. DoD Directive 1100.18, DoD Instruction 1100.19, and DoD 1100.19-H provide guidance and instructions pertaining to the Wartime Manpower Mobilization Planning System (WARMAPS), and direct this Agency to compute and submit wartime mobilization manpower demand and supply requirements.

(b) The DFAS-Headquarters Deputy Director for Resource Management, in coordination with the Deputy Director for Plans and Management, shall develop appropriate wartime manpower mobilization plans for the Agency.

(3) Essential Contractor Service.

(a) According to DoD Instruction 3020.37, it is DoD policy that contractors providing essential service to the Department of Defense will continue to provide such services per the terms and conditions of the contract during periods of crisis, or until appropriately released. Further, DoD

Components working with contractors performing essential services shall develop and implement plans and procedures that provide reasonable assurance of the continuation of essential services during crisis situations.

(b) The DFAS-Headquarters Deputy Directors and Center Directors will comply with the provisions of DoD Instruction 3020.37 and shall submit a report to the DFAS-Headquarters Deputy Director for Plans and Management by December 31 of each year on compliance with the responsibilities and procedures listed in paragraphs E and F of this instruction.

H. EXERCISES.

1. Participation by DFAS in Chairman, Joint Chiefs of Staff (CJCS) Command Post Exercise (CPX).

a. DFAS-Headquarters and Centers actively participate in the Joint Staff CPX program to train staff members regarding contingency responsibilities and requirements, and ensuring that the Agency can support the DoD Components during crisis and emergencies. In support of this program, the DFAS-Headquarters Deputy Director for Plans and Management is responsible for the Agency's planning and execution requirements. The degree of participation will depend upon the exercise scenario. In some cases, the DFAS-Headquarters may support the OSD participation without the Centers' involvement. When the Centers are participating, the Agency CMS will activate. DFAS-Headquarters will publish a support plan for all exercises involving the Centers.

b. The DFAS-Headquarters Deputy Director for Plans and Management, with the assistance of the DFAS-Headquarters Deputy Directors and General Counsel staff, will develop Master Scenario Events Lists (MSELs) for exercises which either identify issues or validate proposed solutions to real world finance and accounting deficiencies. Members of the Contingency Planning Working Group will assist in developing MSELs in support of the Agency's mission and objectives. The participants involved with developing MSELs are "trusted agents" and shall not divulge the information related to the issues evaluated in the exercise. The Agency Director or Principal Deputy Director will review and approve proposed MSELs for CJCS exercises.

c. DFAS-Headquarters will publish a lessons learned report after each CPX based on input from the Centers using the "ISSUE, DISCUSSION, and RECOMMENDATION" format.

2. Agency Exercises. The Agency may conduct in-house, no-prior-notice exercises to test the corporate CMS. The primary purpose is to evaluate personnel notification

procedures and determine the operational status of requisite equipment in the Centers’ CCC.

3. Service Component Exercises. Periodically, some Services will conduct independent command post exercises. DFAS-Headquarters and Centers should participate in these exercises if requested by a Service. Before agreeing to support or participate in a Service exercise, Centers will develop the role DFAS will play in consultation with the DFAS-Headquarters Deputy Director for Plans and Management.

4. Finance Support for Exercises. It is DFAS policy to support Component exercises to the maximum extent possible within available resources. If an installation level Defense Accounting Office/Defense Military Pay Office does not have the resources to support an exercise, advise the requester to contact the parent DFAS Center for support.

I. REMEDIAL ACTION PROJECT (RAP) PROGRAM. The RAP program tracks the finance and accounting problems/issues and other related items resulting from command post exercises, Service deployments, operations, training exercises, and other assessments or reviews. This program consists of a written description of a deficiency or shortcoming in existing policies, supporting strategies, plans, procedures, systems, material or personnel for correction by specific actions. Furthermore, the program assigns corrective action and tracks the problem until completion and validation of corrective action. The DFAS RAP program is described at Appendix C.

J. CRISIS ACTION PACKAGES (CAPs). Crisis Action Packages are a set of documents that facilitate the assembly of essential elements of information and provide specific guidance on likely issues and decisions to make recommendations to the Director, DFAS and other DFAS officials during a crisis. Each CAP contains background information on legal authorities and coordination requirements as well as draft copies of specific implementing documents that can be quickly adapted in response to an emergency. Guidance on preparation of CAPs is at Appendix B.

APPENDIX A

SITUATION REPORTS

A. PURPOSE. These instructions establish the Defense Finance and Accounting Service (DFAS) policies, procedures, and responsibilities for the DFAS Situation Report (SITREP) reporting system.

B. GENERAL.

1. The DFAS Situation Report (SITREP) reporting system is the means by which the Centers and OPLOCs notify the Director, DFAS and DFAS-Headquarters Deputy Directors of significant events. The purpose is to keep DFAS-Headquarters continually apprised of important situations occurring within the DFAS network. Provide DFAS-Headquarters a SITREP for events that have or could adversely impact the mission or negatively impact on the reputation of the Agency; information during an actual contingency operation or exercise, and significant incident reports on counter intelligence, fraud and criminal matters that meet the reporting thresholds in DoD Instruction 5240.4.

2. The key to the success of the SITREP is prompt reporting of information to DFAS-Headquarters. If complete details are not available, promptly report the information available and follow-up with additional information as it becomes available.

3. Normally, the SITREP is a written report. The SITREP format is at Figure A-1. However, the time sensitive nature of some information may necessitate an initial telephonic report to DFAS-Headquarters.

4. OPLOCs will forward SITREPs through their parent Center. However, if the OPLOC Director feels that DFAS-Headquarters must immediately have the information in the SITREP, forward an information copy of the SITREP to DFAS-Headquarters.

5. Submission of a SITREP does not supersede or replace other normal reporting requirements for: safety, casualty, criminal, damage assessment, and security violations etc.,. The SITREP is a supplement that serves as a vehicle to provide quick information to DFAS-Headquarters.

7. Protect and classify SITREPs according to the sensitivity of the information they contain. Transmit classified information and unclassified information considered sensitive or deserving of protection from uncontrolled dissemination according to applicable security directives and your activities respective Automated Information System (AIS) Security Plan.

C. RESPONSIBILITIES.

1. DFAS-Headquarters.

a. Deputy Director for Plans and Management (DFAS-HQ/M) will:

(1) Implement the DFAS SITREP system within DFAS according to this appendix.

(2) Establish appropriate files and procedures to ensure that SITREPs are properly recorded and distributed for action and information to DFAS-HQ Deputates.

(3) Forward SITREPs to OSD officials when directed by the Director or his representative.

(4) Activate Center and OPLOC daily SITREP reporting, when required, during contingency operations and exercises.

(5) Terminate Center and OPLOC daily SITREP reporting when the crisis subsides or exercise ends.

b. Deputy Directors shall:

(1) Provide the DFAS-HQ CCC with a point-of-contact for distribution of SITREPs.

(2) Review SITREPs pertaining to their functional area, initiate support action as required, and if appropriate, recommend forwarding SITREPs for review by the appropriate OSD officials.

2. Center and OPLOC Directors shall:

a. Establish local procedures to identify, record and report situations addressed in these instructions.

b. Provide SITREPs to DFAS-Headquarters within 48 hours of an incident.

c. Forward SITREPs via the fastest means possible.

d. Establish a central contact point, normally the Center or OPLOC CCC, to assist with follow-on requests for information without disrupting normal operations. Provide DFAS-HQ/M with points of contact -- name(s) and phone numbers (both home and work).

e. Recommend SITREPs for distribution to OSD officials, if deemed appropriate.

f. Provide follow-on reports, normally on a daily basis, listing all significant changes until resumption of normal operations or until directed to terminate reporting.

g. Submit daily SITREPs on operations in support of contingencies or exercises, when directed by DFAS-HQ/M.

h. Report unusual situations not warranting a SITREP to the Office of Primary Interest.

3. The FSO shall submit SITREPs when reportable situations occur at the FSO or any of the Financial Systems Activities (FSA).

D. REPORTING REQUIREMENTS.

1. Significant Events or Conditions. Centers and OPLOCs will submit a SITREP to DFAS-Headquarters if:

a. The situation has or could have a significant negative impact on mission accomplishment and may require DFAS-HQ assistance. Forward a SITREP whenever any of the following occurs:

(1) Continuity of Operations. Report interruptions in normal operations of **four or more hours** for unplanned equipment/power failure or other unprogrammed reasons such as bomb threats, weather and strike/work stoppage. Examples of equipment or power failure are: phone outage, non availability of on-line financial or pay systems and/or delayed processing of batch products at DMC and IPCs due to equipment and/or communication network failure; and Enterprise Local Area Network (ELAN) problems affecting the Center and/or subordinate organizations.

(2) Adverse Publicity. Incidents that may receive significant media coverage or Congressional interest.

(3) Criminal and Fraud Activities: Report to Headquarters actual or possible criminal cases and allegations of fraud identified at DFAS activities. Take special care to limit access to sensitive information related to on going investigations of these activities. Provide periodic updates to

the SITREP including a final report outlining the investigation result.

(4) Death, Occupational Injuries or Hospitalization of DFAS Employees, or Members of the Public. Report all deaths, injuries or hospitalization of key DFAS management associates. In addition, report job related incidents classified as either Class A or B mishaps:

(a) Class A Mishap: Death or permanent total disability of an employee, hospitalization of 5 or more persons, or resources loss or damage over $1 million.

(b) Class B mishap. Permanent partial disability, temporary total disability more than 3 months, hospitalization of 3 or more persons, or resource loss or damage over $200,000 but less than $1 million.

(5) Emergency Assistance Requests. Report emergency assistance required by, or provided to, another DoD Component or Federal Agency.

(6) Terrorist Activities. Report any terrorist activity including instances of sabotage or espionage.

b. Actual Contingency Operations and Exercises. When directed by the DFAS-Headquarters, the Centers and OPLOCs will submit SITREPs regarding their support to contingency operations and/or exercises.

c. SITREPs forwarded by Headquarters-DFAS to the Office of the Secretary of Defense. When requested by OSD officials or directed by the Director, DFAS, the DFAS-HQ Deputy Director for Plans and Management will forward certain SITREPs to the appropriate OSD officials. DFAS-HQ/M will forward SITREPs on counter intelligence, fraud and criminal matters that meet the reporting thresholds under DoD Instruction 5240.4 after review and approval for release by the DFAS Director or his designated representative.

2. SITREP Reports.

a. Unclassified SITREPs. Prepare and forward a SITREP by cc: Mail to the DFAS-HQ/CCC mailbox in the format at figure
A-1 when an incident occurs or becomes known.

b. Classified or Sensitive SITREPs. Transmit unclassified or sensitive information through the Secure Wide Area Net (SWAN). If the SWAN is not available, transmit the SITREP by secure facsimile. Transmission by secure facsimile is possible only when someone is available at the DFAS-HQ CCC.

c. Telephonic SITREPs. In the event extenuating circumstances preclude the development of a written SITREP on a situation requiring an immediate report, provide DFAS-HQ an initial telephonic SITREP.

(1) Make preliminary telephonic reports immediately to the DFAS-HQ CCC, during normal duty hours of 0730-1630 Eastern Standard (Daylight) Time, Monday-Friday.

(2) If an incident occurs during non duty hours, make the report to the DFAS-HQ CCC Duty Officer according to the instructions to be developed separately by the DFAS-Headquarters, Deputy Director for Plans and Management.

Figure A-1
SITREP FORMAT

1. DFAS-HQ SITREP # __________2. Cover Brief Prepared? Yes/No

3. Meets Significant Incident Report Reporting Threshold? Yes/No

4. From: _____________   5. Center SITREP #________

6. Date & Time of Report: ___________________

7. Reporter Name: ____________Location: ___________
Phone #:_______

8. Follow-up Point of Contact & Telephone #:_____________

9. Date & Time of Situation/Incident: _______________

10. Site(s):__________11. Report Type: Initial/Update/Final

12. Nature of Situation/Incident: __________________________
____
____
____
____

13. Narrative Description of Situation/Incident: _______
____
____
____

14. Brief Explanation of Mission Impact/Why Significant?:
____
____
____

15. Corrective Action Initiated and Estimated Completion Date:
____
____
____
____

16. Type of Assistance Requested from Headquarters, if any:
____

17. Real/Potential Adverse Publicity/News Media coverage:
____

18. Individual(s) Involved:____________________________

19. Investigating Organization, Investigator & Telephone #:
____

20. Name of System(s) Involved: ___________________________

21. DMC or IPC:
    a. Name: _____________
    b. POC: _____________
    c. Telephone #: __________
    d. Trouble Ticket #: _________

22. System Downtime Hours: ________________

23. Dollars Involved: __________________

APPENDIX B

CRISIS ACTION PACKAGES (CAPs)

A. PURPOSE

This appendix:

1. Establishes the DFAS CAP system to enhance training, readiness posture and continuity.

2. Establishes policy and prescribes procedures for development and maintenance of the CAPs and provides for general administration of those packages.

2. DEFINITION.

Crisis Action Package. A set of documents that facilitate the assembly of essential elements of information and provide specific guidance on likely issues and decisions that could confront the Director, Defense Finance and Accounting Service and other DFAS officials during a crisis. Each CAP contains background information on legal authorities and coordination requirements as well as draft copies of specific implementing documents than can be quickly adapted in response to an emergency.

C. REFERENCE. DOD Instruction 3020.38, “ Promulgation and Administration of OSD Crisis Action Packages (CAPs)” , December 13, 1990.

D. POLICY.

It is DFAS policy that:

1. Each DFAS organization shall share the general responsibilities for crisis management preparedness, planning and execution.

2. CAPs should focus on those potential crisis-related events that could require rapid development of a DFAS position on which to base recommendations to the leadership.

3. An integral part of each CAP are alternatives, processes and issues considered during various stages of national security emergencies.

E. RESPONSIBILITIES.

1. The DFAS-Headquarters, Deputy Director for Plans and Management shall:

a. Establish and promulgate CAP system policy.

b. Designate DFAS-HQ proponents for CAPs applicable DFAS-wide.

2. The CAP proponents shall:

a. Develop and maintain CAPs necessary to provide, on no notice or short notice, the information required to develop accurate and timely recommendations.

b. Review their responsibilities as established in Chapter 1, DFAS 3020.26-R, Corporate Contingency Plan and supplements to the Corporate Contingency Plan by July 1 of each year. Develop all necessary CAPs and ensure that all existing CAPs are current and in compliance with this Appendix.

c. Ensure the accuracy, objective content and completeness of CAPs.

d. Submit each CAP to the supporting General Counsel to ensure legal sufficiency.

e. Maintain an historical file and background on each CAP for which they are responsible.

f. Determine classification, downgrading and declassification markings in accordance with information security program regulations.

g. Review CAPs after each crisis and before each major exercise (at least annually) to ensure information and procedures are correct.

F. PROCEDURES.

1. Review CAPs semiannually during the months of June and December. The proponent for the CAP shall perform the review.

2. Administratively reissue CAPs every 3 years whether or not interim changes were made to the basic document.

3. Format for the Crisis Action Packages is at Figure B-1.

Figure B-1

FORMAT FOR CRISIS ACTION PACKAGES

TITLE:

DFAS PROPONENT:

DECISION LEVEL:

PURPOSE:

BACKGROUND:

LEGAL AUTHORITIES

PREREQUISITE ACTIONS:

ACTION REQUIRED:

ALTERNATIVES:

IMPACT ON OTHER ACTIONS:

EXPECTED BENEFITS:

EXPECTED COSTS:

RELATED ACTIONS:

INTERNAL COORDINATION REQUIRED:

EXTERNAL COORDINATION REQUIRED:

TABS:

APPENDIX C

REMEDIAL ACTION PROJECT (RAP) PROGRAM

A. **PURPOSE**.

This appendix establishes policy, assigns responsibilities, and prescribes procedures for the Agency Remedial Action Projects program.

B. **DEFINITION**.

Remedial Action Project (RAP) Program. The remedial action projects program tracks the finance and accounting problems/issues and other related items resulting from command post exercises, deployments, operations, training exercises, and other assessments or reviews. This program consists of a written description of a deficiency or shortcoming in existing policies, supporting strategies, plans, procedures, systems, material or personnel for correction by specific actions. Furthermore, the program assigns corrective action and tracks the problem until completion and validation of corrective action.

C. POLICY. The objectives of the program are:

1. Identify real-world finance and accounting impediments to the Defense Department’s total force war fighting capability.

2. Assign responsibility for corrective action.

3. Review and track status of corrective actions taken to solve an identified problem.

4. Evaluate the effectiveness of the corrective actions.

5. Identify other deficiencies for correction through the CJCS RAP program by either the Joint Staff, Military Services, unified and specified commands, OSD, DOD Agencies, or other Federal Agencies.

D. **RESPONSIBILITIES**.

1. The DFAS-Headquarters Deputy Director for Plans and Management shall:

   a. Establish and promulgate RAP policy.

   b. Recommend RAPs for completion to the Director.

2. The DFAS-Headquarters Director for Planning and Management Support, Plans and Management Deputate shall:

a. Manage the DFAS RAP program.

b. Ensure identification and integration of lessons learned, that are not RAP items, into the corporate business practices.

c. Maintain the database of remedial project information.

d. Include events to exercise Master Scenario Events List (MESL) to validate closed RAPs.

3. The DFAS-Headquarters Deputy Directors and General Counsel shall:

a. Fully support the RAP program.

b. Designate representatives for the DFAS-HQ Contingency Planning Working Group.

c. Assign a point of contact for each RAP when designated as the office of primary responsibility (OPR) and office of secondary responsibility (OSR).

E. **PROCEDURES**.

1. The RAP program procedures include identifying and categorizing possible issues, accepting recommended RAPs into the program, assigning an office of primary responsibility (OPR) and the office of secondary responsibility (OSR) to correct the problem, monitoring progress until completion of actions, validating solutions, and closing the remedial action project.

a. Problem Identification. Any person can identify a finance and accounting problem or related item. Principal sources are real world operations, CJCS command post exercises, corporate no-notice inter-operability exercises, and training exercises.

b. Issue Categorization. After receipt of a written issue, the DFAS-HQ Director for Planning and Management Support will staff the item to members of the DFAS-HQ Contingency Planning Working Group for review. The Working Group will: 1) ensure identification of all elements of the issue, 2) ensure the issue has a complete write-up, 3) determine if the item meets the RAP criteria for corporate action or a joint solution, and 4) if it meets the RAP critieria categorize as one of the following lessons learned:

(1) Procedure Item. Procedures exist but not followed. Corrective action is not necessary and the item only serves to identify potential areas for training and increased command attention.

(2) Exercise Item. Items that only pertain to exercise design or management.

(3) Noted Item. Items that do not require corrective action or an established program exists that is already addressing the issue. Noted items include positive comments about procedures, systems, techniques, etc., that worked well.

2. The DFAS-Headquarters Deputy Director for Plans and Management will staff the write-ups to the DFAS-Headquarters Deputy Directors and General Counsel for concurrence and the assignment of an office of responsibility for those items categorized as RAPs.

3. The DFAS-HQ Director for Planning and Management Support will disseminate lessons learned or items not meeting the RAP criteria to the appropriate office.

4. Assign each approved RAP a DFAS control number used until resolution of the identified problems. DFAS-HQ Director for Planning and Management Directorate Support will maintain an updated database file on each remedial project with sufficient detail to identify the issues and proposed solutions. Forward issues that meet the CJCS criteria for joint service action to the Vice Director, J-7, through the Office of Deputy Under Secretary of Defense for Policy (Security Policy) using Joint Universal Lessons Learned (JULLS) software.

5. The DFAS-Headquarters OPR shall develop a plan of action and milestones for each assigned RAP. Furthermore, the OPR should form action or working groups to include Service and organization representatives as appropriate to ensure consideration of joint/common solutions. The OSR should work closely with the OPR in developing a plan of action and milestones and provide the required assistance until validation of a solution. If a non-DFAS organization should be the appropriate OSR, the DFAS OSR should request that office assume responsibility for the RAP before reflection of the assignment in the write-up.

6. The OPR will provide individual RAP updates to DFAS-Headquarters Director for Planning and Management Support as follows:

a. At least every six months on May 31 and November 30.

b. Within 30 days after a scheduled milestone completion. If the scheduled milestone was not met, the update should contain an explanation of the reason for the delay.

c. When the OPR wants to document changes in the RAP (e.g. when a new input, designated as a fold-in, significantly alters the RAP status).

d. When the OPR wishes to report that action is completed.

e. When requested by DFAS-Headquarters Deputy Director for Plans and Management.

7. After receipt of status updates, DFAS-Headquarters Director for Planning and Management Support will incorporate the changes in the RAP database. The DFAS-Headquarters Deputy Director for Plans and Management will provide a status report for the Director’s approval on June 30 and December 31 to inform the Agency’s staff, Military Departments financial managers and other organizations of the status of finance and accounting issues.

8. As new exercises or as operations occur, identify additional issues that are similar to existing RAPs. The DFAS-Headquarters Contingency Planning Working Group will review these similar items and integrate them into existing RAPS as appropriate, with the approval of the OPR.

9. When an OPR determines that all necessary actions are complete by his organization but more work is necessary, transfer the RAP to another office based on agreement by the two parties.

10. After ensuring that all required actions to solve a problem are complete, the OPR Deputy Director will forward a RAP status report update to DFAS-HQ Deputy Director for Plans and Management, stating completion with a recommendation for closure of the RAP. If the DFAS-HQ Deputy Director for Plans and Management concurs, forward the recommendation to the Director, DFAS for approval. In most cases, the approval is conditional, based on completion of a satisfactory validation test.

11. An effective correction action requires validation of the recommended solution. A CJCS exercise is the most common vehicle for RAP validation. Therefore, OPRs should coordinate with the DFAS-HQ Director for Planning and Management Support to add the appropriate events to the Master Scenario Events List (MSEL) for these exercises. Other acceptable means of validation include CINC sponsored exercises or studies demonstrating problem resolution. Should the RAP validation be unsuccessful, or not completed due to scenario constraints, OPRs must provide an updated status report with the new recommended validation schedule.

12. Close a RAP when any of the following occurs:

a. Action is completed and validated.

b. Action is completed and validation is not required.

c. Corrective action to remedy the problem was repeatedly unsuccessful (e.g. legislative actions fail, budget requests, policies, or recommended actions are disapproved).